Співпраця з KPMG

—

Давайте зробимо це

Working with KPMG– v.3

Ми робимо те, що правильно: Порядність у всьому - KPMG - 2023

Глобальний кодекс поведінки

Наші цінності

Не мовчимо!

Система прийняття етичних рішень – CARE

CEAC

Виконання завдань

Недопущення хабарництва

Конфіденційна інформація

Недопущення інсайдерської торгівлі

Незалежність

Вимоги до звітування

Клікніть на кожній іконці, щоб дізнатися більше.

Посилання на політики KPMG доступні тільки для підрядників з акаунтом KPMG

Наша культура етичної поведінки та співпраці

Створена у KPMG культура етичної поведінки та співпраці має вирішальне значення для формування довіри для нашої фірми і досягнення наших планових показників зростання, а також довгострокового ділового успіху.

- Ця культура допомагає нам наймати найкращих співробітників і бути саме тим місцем роботи, де ***вам*** хочеться працювати.
- Наша культура лежить в основі наших відносин з клієнтами, організаціями, в яких проводиться аудит, регулюючими органами, стратегічними партнерами, постачальниками та іншими зацікавленими сторонами.
- Вона підтримує довіру до нас з боку наших клієнтів, співробітників та зацікавлених сторін і суспільства в цілому. А довіра має важливе значення для прискорення нашого зростання та збільшення частки ринку.

Наша відданість неухильному дотриманню наших цінностей очевидна: ***ніколи*** не може виникнути ситуація, ні всередині, ні за межами роботи KPMG, де було б прийнятним порушення наших стандартів поведінки.

Наша культура етичної поведінки та співпраці стає міцнішою, коли ми всі беремо на себе особисту відповідальність за дотримання наших цінностей у всьому, що ми робимо, і очікуємо такої ж відповідальної поведінки один від одного.

Глобальний кодекс поведінки

Глобальний кодекс поведінки (далі – «Кодекс») прописує, як ми повинні діяти на роботі та в житті. Він включає в себе такі розділи:

- **Цінності KPMG**
- **Зобов’язання KPMG**
- **Обов’язки KPMG**
- **До кого звертатися за допомогою**
- **Дотримання Кодексу поведінки**

Кодекс чітко визначає етичні стандарти поведінки, яких повинні дотримуватися всі співробітники KPMG. Кодекс роз'яснює, що означає працювати в KPMG і бути частиною фірми, а також детально висвітлює наші особисті та колективні обов'язки та зобов'язання

Більш детальна інформація наведена за посиланнями:

- Глобальний кодекс поведінки
- 5.6.1 Дотримання законів, нормативних актів і професійних стандартів

Цінності KPMG: у що ми віримо

Меню

Integrity

Ми робимо те, що правильно

Excellence

Ми ніколи не припиняємо вчитись та вдосконалюватись.

Courage

Ми мислимо та діємо сміливо.

Together

Ми поважаємо одне одного і знаходимо силу в наших відмінностях.

.

For Better

Ми робимо те, що справді важливо.

Натисніть на кожне посилання, щоб дізнатися більше

Більш детальну інформацію про наші цінності можна знайти за посиланням

Integrity (порядність у всьому)

Ми робимо те, що правильно.

Меню

Натисніть тут, щоб повернутися до першого слайду по темі "Цінності KPMG"

Що це означає?

- Стійке керівництво іншими людьми на основі особистого прикладу з дотриманням високих стандартів і моральних норм
- Чесність і правдивість у словах і вчинках
- Здатність протидіяти тиску у складних умовах, зберігаючи при цьому чесність

Порядність означає, що ми чесні, справедливі та **послідовні** в своїх заявах, діях і рішеннях — як у своїй роботі, так і в тому, що з нею не пов’язане. Ми несемо **відповідальність** за свої дії в повсякденному житті і завжди співвідносимо свої вчинки з **найвищими стандартами моралі та етики**, навіть коли опиняємося в складних ситуаціях і відчуваємо тиск **ззовні**. Ми дотримуємося слова та подаємо приклад іншим.

Основні теми

Чесність, справедливість, виконання обіцянок, відповідальність

Excellence (бездоганна якість)

Ми ніколи не припиняємо вчитися та вдосконалюватися.

Меню

Натисніть тут, щоб повернутися до першого слайду по темі "Цінності KPMG"

Що це означає?

- Встановлення стандартів якості та їх дотримання
- Постійне вдосконалення поточної діяльності та розвиток корпоративної культури
- Готовність нести відповідальність за свої дії

Бездоганна якість має на увазі постійне забезпечення якості послуг, що **відповідає найвищим професійним стандартам.** Ми приділяємо пильну увагу всім о**станнім змінам і несемо особисту відповідальність за підвищення своєї професійної обізнаності.** Ми прагнемо безперервно підвищувати якість своєї роботи, для чого вивчаємо **нову інформацію та різні точки зору, готові приймати нові виклики і раді отримувати зворотний зв'язок,** оскільки саме такий підхід дає нам можливість розвиватися і підвищувати наш професійний рівень

Основні теми

Якість, професійні стандарти, вихід за рамки, безперервне навчання

Courage (долаємо нові виклики)

Ми мислимо та діємо сміливо.

Меню

Натисніть тут, щоб повернутися до першого слайду по темі "Цінності KPMG"

Що це означає?

- Чесність і прямота у відносинах
- Відкритість до інновацій і нових ідей
- Постійне прагнення виділятися на ринку

Сміливість означає **готовність сприймати нові ідеї і чесне визнання** того, що наші знання і досвід не є істиною останньої інстанції. Сміливість означає, що ми повинні **проявляти професійний скептицизм** і не боятися **ставити питання, якщо у нас виникають сумніви.** Ми **не мовчимо,** коли на наших очах відбувається щось таке, що ми вважаємо неправильним, і **підтримуємо тих, хто проявляє сміливість та відверто висловлює свою думку.**
Іншими словами, сміливість – це **готовність** без вагань вийти із зони комфорту.

Основні теми

Відкритість, зворотний зв'язок, інновації, впевненість

Together (сила у різноманітті та унікальності в командній роботі)

Меню

Натисніть тут, щоб повернутися до першого слайду по темі "Цінності KPMG"

Ми поважаємо одне одного і знаходимо силу в наших відмінностях.

Що це означає?

- Проявлення турботи й уваги до інших людей
- Забезпечення соціокультурного різноманіття та врахування індивідуальних особливостей
- Співпраця всередині команди та між командами

Максимальний за якістю та змістом результат можливий тільки тоді, коли для його досягнення ведеться **спільна робота** – спеціалістів у команді, декількох команд, а також з людьми поза межами організації. Важливість співпраці полягає ще і в тому, що саме вона **формує думки** і стимулює творчий підхід до справи. Пліч-о-пліч з нами працюють люди з **різних** країн, яким притаманні **різні** вміння, які дотримуються **різних** точок зору та мають **різний** досвід, тому ми робимо все можливе, щоб чути думку кожного з них. Ми **уважно та з повагою** ставимося до всіх наших працівників і прагнемо до створення **робочої атмосфери**, яка дає їм можливість відчути себе частиною єдиного цілого.

Основні теми

Співпраця, врахування індивідуальних особливостей, турбота, залученість

For Better (сприяємо позитивним змінам)

Ми робимо те, що справді важливо

Меню

Натисніть тут, щоб повернутися до першого слайду по темі "Цінності KPMG"

Що це означає?

- Задоволення потреб і зміцнення наших ринків і спільнот
- Прагнення зробити фірму кращою, щоб вона приносила користь майбутнім поколінням
- Позитивний вплив на життя суспільства

Позитивні зміни означають, що вся наша робота ведеться **з розрахунком на майбутнє**. Саме цієї точки зору ми дотримуємося, коли приймаємо рішення, які є актуальними тут і зараз, оскільки хочемо додатково **зміцнити фундамент, на якому KPMG будуватиме свою роботу в майбутньому**. Ми завжди пам'ятаємо про важливість нашої ролі у **зміцненні довіри** на світових ринках капіталу та в бізнес-середовищі. Ми вносимо **позитивні зміни** в життя місцевих громад і суспільства в цілому і сподіваємося, що в майбутньому ці зміни **зроблять наш світ кращим**.

Основні теми

Довгострокове бачення, відповідальне планування та управління, суспільство, мета

Інформування про можливі порушення

Ви зобов'язані повідомляти про потенційні або здогадні порушення політики KPMG, чинного законодавства або професійних стандартів. Це включає випадки, коли ви знаєте або підозрюєте, що ваш(-а) колега/колежанка, клієнт KPMG або особи, пов'язані з клієнтом, постачальником, субпідрядником або іншими третіми особами, пов'язаними з фірмою, залучені або можуть бути залучені до протиправних дій чи будь-якої діяльності, що порушує етичні норми. У KPMG ви можете повідомляти про можливі порушення і порушувати питання без страху санкцій у відповідь, які для нас є категорично неприйнятними у будь-якій формі, і для вирішення цієї проблеми буде вжито відповідних заходів.

Див. детальнішу інформацію у розділах 5.6.2 Повідомлення про порушення з боку клієнтів або третіх сторін, 5.6.3 Повідомлення про порушення з боку фірми-члена мережі KPMG або її персоналу та 14.2.6 Процес повідомлення про підозрюване недотримання законів і нормативних актів або політик KPMG.

KPMG пропонує велику кількість каналів комунікації, щоб отримати рекомендації та обговорити сумніви, що виникають. Ви ніколи не залишитеся сам на сам з етичною дилемою.

Розв'язати проблему найкращим чином, як правило, можуть найбільш близькі до ситуації люди (наприклад, партнер із завдання). Залежно від ситуації, ви можете також розглянути інші канали зв'язку. Завжди обирайте той канал, який є для вас найбільш зручним. Головне, щоб ви не мовчали!

- Супервайзер, менеджер підрозділу або менеджер-куратор
- Партнер із завдання
- Партнер з питань етики та незалежності (EIP)
- Партнер з управління ризиками (RMP)
- Гаряча лінія KPMG International (KPMGI Hotline)
- Інші канали передавання інформації поза межами вашої фірми

Інформування про можливі порушення

Менеджер проєкту / контактна особа KPMG

Звертайтеся до менеджера проєкту або контактної особи з KPMG, щоб обговорити питання або проблемні моменти, з якими ви зіткнулися. Ви також можете повідомити про неправомірну поведінку, яка потребує реагування або ескалації.

Партнер із завдання

Звертайтеся до свого партнера із завдання щодо питань, які стосуються його або її клієнтів, у тому числі: (1) недотримання законів або нормативних актів клієнтами або третіми особами та (2) порушення політики KPMG або недотримання законів, нормативних актів або професійних стандартів фірмами-членами мережі KPMG або їх персоналом.

Партнер з питань етики та незалежності (EIP)

Звертайтеся до свого EIP у разі порушень, пов'язаних з питаннями етики та незалежності з боку фірм-членів KPMG або їх персоналу.

Про порушення політики щодо незалежності слід повідомляти негайно.

Партнер з управління ризиками (RMP)

Звертайтеся до свого RMP з питань, що не стосуються клієнтів (так само, як ви зазвичай повідомляєте про питання, пов'язані з клієнтами, партнеру із завдання). Якщо ви вважаєте, що партнер із завдання якимось чином причетний до справи або не вирішує питання належним чином, зверніться до свого RMP.

Інформування про можливі порушення

Гаряча лінія KPMG International (KPMGI Hotline)

KPMGI Hotline є доступною, і ви можете скористатися нею, якщо ви відчуваєте незручність або маєте сумніви щодо використання каналу зв'язку всередині вашої фірми-члена мережі KPMG.

KPMGI Hotline управляється персоналом KPMG International і забезпечує конфіденційність та анонімність повідомлень.

Інші канали передавання інформації поза межами вашої фірми

Додатково до осіб, які підтримують KPMGI Hotline, нижче наведено перелік інших осіб, що не є співробітниками вашої фірми, до яких можна звернутися за допомогою :

- Відділ глобального управління якістю та ризиками
- Міжнародний офіс Генерального юридичного консультування
- Ваш Регіональний партнер з управління ризиками

Система прийняття етичних рішень – CARE

Розглянути

В чому полягає проблема?

- Чи може дана ситуація зашкодити команді, клієнту або нашій репутації?
- Чи було б прийнятно, якби так вчиняв кожен співробітник KPMG?
- Якими фактами ви володієте і які додаткові факти вам потрібні для прийняття обґрунтованого рішення?
- Які правила, положення або політики KPMG вам необхідно взяти до уваги?

Проаналізувати

варіанти вирішення ситуації

- Чи відповідають запропоновані вами дії Цінностям KPMG та нашому Кодексу поведінки?
- Які існують ризики? Як ви їх мінімізуєте?
- Який тиск, раціональні міркування та упередження можуть вплинути на ваше рішення? Як ви будете реагувати на них?
- Який вплив запропоновані вами дії матимуть на інших, у тому числі на вашу команду, клієнтів і нашу фірму?
- Чи існує ризик того, що запропоновані вами дії можуть бути сприйняті не так, як ви планували?
- Чи почуватиметеся ви комфортно, якщо ваша відповідь стане відомою широкому колу осіб?

Відповісти

Прийняти рішення

- Яке ваше рішення?
- Чи зручно вам підтримувати своє рішення, якщо його оскаржать, чи вам потрібно проконсультуватися??
- Кому вам треба повідомити про своє рішення (наприклад, вашій команді, клієнтам, нашій фірмі, регуляторам)?
- Як ви поясните їм своє рішення?
- Чи потрібно вам задокументувати своє рішення?

Розвиватися

та обміркувати

- Чому ви навчилися в процесі прийняття рішень?
- Які існують можливості поділитися отриманим досвідом?
- Як ваше рішення вплинуло на інших, включаючи вашу команду, клієнтів та нашу фірму?
- Чи ви зробили б щось інакше?

Радьтеся та комунікуйте – у будь-якій точці

CEAC

Те, з ким ми працюємо і що ми робимо, має значення

Важливо, щоб кожен з нас розумів, що ми несемо спільну відповідальність згідно з Кодексом поведінки та нашим Планом впливу за те, щоб наші рішення щодо клієнтів та завдань відповідали нашим бізнес-стратегіям, нашим цінностям та етичним принципам.

Наша політика управління ризиками та процеси прийняття нового клієнта та завдання і продовження відносин з клієнтом (CEAC) допомагають нам орієнтуватися в цих рішеннях і робити правильні висновки.

Працюючи разом над тим, щоб забезпечити виконання процесів CEAC, та ретельно зважуючи наші рішення щодо клієнтів та завдань, ми підтримуватимемо та розвиватимемо наш бренд на світовому ринку та реалізуємо наші амбіційні плани щодо укрaплення довіри та зростання бізнесу.

Якщо у вас виникли запитання або стурбованість щодо того, що рішення про прийняття клієнта та/або завдання чи продовження відносин з клієнтом не відповідають нашим Цінностям, ви зобов'язані повідомити про це, скориставшись одним із багатьох доступних каналів зв'язку.

Виконання завдань

Натисніть тут, щоб повернутися до першого слайду по темі "Виконання завдань"

Відстоювання наших Цінностей (Integrity, Excellence, Courage, Together, і For Better) дозволить вам з гордістю служити нашим клієнтам та суспільним інтересам.

Нижче наведені певні міркування щодо роботи над завданнями.

Бути пильними

Відстежувати проблеми

Проявляти професійний скептицизм

Документувати

Уникати упередженості

Натисніть на кожне з полів, щоб дізнатися більше.

Виконання завдань

Натисніть тут, щоб повернутися до першого слайду по темі "Виконання завдань"

Бути пильними

Якщо у вас виникли сумніви або ви підозрюєте, що щось не так, будьте скептичними – не вірте всьому, що вам кажуть. Продовжуйте ставити запитання, доки не переконаєтеся, що проблема була вирішена належним чином.

Про потенційні проблеми, що стосуються персоналу клієнта або інших осіб у вашій фірмі-члені мережі KPMG, слід негайно повідомляти вашому партнеру із завдання або RMP.

Виконання завдань

Натисніть тут, щоб повернутися до першого слайду по темі "Виконання завдань"

Відстежувати проблеми

Завжди відстежуйте потенційні проблеми. Переконайтеся, що всі питання належним чином оцінені, а всі вимоги щодо звітування виконані.

Виконання завдань

Натисніть тут, щоб повернутися до першого слайду по темі "Виконання завдань"

Проявляти професійний скептицизм

Не слід беззастережно вірити версії клієнта!

Приклади ситуацій з клієнтами, в яких ви повинні ставити запитання, включають:

- Використання агентів для здійснення платежів у середовищах або галузях з високим рівнем ризику, таких, як видобуток природних ресурсів, будівництво, оборона та фармацевтика, або в юрисдикціях з високим ризиком корупції.
- Вимога до KPMG використовувати певних третіх осіб, таких, як конкретний субпідрядник, для виконання завдань.
- Нещодавнє звільнення поточних аудиторів суб'єкта господарювання протягом місяця після кінцевого терміну подачі ними конкурсних документів.
- Укладення значних комерційних контрактів (наприклад, контракт на будівництво нової будівлі або укладення великого державного контракту в юрисдикції з високим ризиком корупції) без відкритого (або будь-якого) конкурсу.
- Бізнес-модель та операції є незрозумілими, включають холдингові компанії та юридичних осіб спеціального призначення, розташованих у відомих податкових гаванях
- Неможливість забезпечити підтримку великих регулярних платежів третій стороні.

Отримайте належні докази на підтримку оцінки та висновків, зроблених вами та вашою командою із завдання щодо цих подій.

Виконання завдань

Натисніть тут, щоб повернутися до першого слайду по темі "Виконання завдань"

Документувати

Робочі документи повинні документувати виявлені вами проблеми, отримані докази та їхнє вирішення, щоб не залишалося неопрацьованих питань.

Подумайте, чи варто залучати внутрішнього юриста до перегляду та доопрацювання робочих документів.

Виконання завдань

Натисніть тут, щоб повернутися до першого слайду по темі "Виконання завдань"

Уникати упередженості

Будьте обережні, не допускайте упередженості при оцінці питань та прийнятті рішень. Не припускайтеся помилки, вважаючи, що клієнт або люди, яких ви знаєте, ніколи не можуть бути причетними до хабарництва, корупції, будь-яких інших незаконних або неетичних дій або будь-якої іншої діяльності, яка може завдати шкоди бренду KPMG.

Хабарництво

KPMG категорично не приймає будь-яку форму хабарництва або корупції з боку співробітників KPMG або сторін, з якими ми можемо мати справу. Ми зобов'язуємося вести свій бізнес чесно, з урахуванням етичних норм і намагаємося уникати навіть найменшого натяку на те, що KPMG або будь-який з наших співробітників міг запропонувати або взяти хабар з метою отримання будь-якої переваги.

Слідкуйте за тим, щоб пропонування або отримання подарунків чи розваг не ставило під сумнів чесність, незалежність, об'єктивність або професійне судження – ваше або KPMG.

Для більш детальної інформації див. такі політики:

- 5.7.1 – Заборона на причетність до хабарництва
- 5.7.2 – Винагорода за "спрощення формальностей"
- 5.7.3 – Заохочення, включаючи подарунки та розваги

проконсультуйтеся з політикою щодо подарунків та розваг вашої фірми-члена мережі KPMG, щоб отримати додаткові інструкції щодо місцевих вимог, включаючи відповідні обмеження

- 14.4.1 – Відповідні кроки з протидії хабарництву у відносинах з організаціями-постачальниками
- 14.4.2 – Внутрішній контроль у рамках протидії хабарництву
- 14.4.6 - Оцінювання фірми-учасника мережі KPMG на предмет протидії хабарництву та корупції
- Які ми? - KPMG Ukraine Антикорупційна програма KPMG

Конфіденційна інформація

Більша частина інформації, що створюється, збирається та передається KPMG, є тією чи іншою мірою конфіденційною, і кожному співробітникові відведена важлива роль у її захисті

За жодних обставин ви не повинні використовувати цю інформацію у своїх власних інтересах або в інтересах інших осіб, розголошувати її поза межами KPMG або ділитися нею з працівниками фірми, в яких відсутня службова необхідність використовувати цю інформацію.

Дотримуйтеся політик і процедур KPMG для захисту конфіденційної інформації в будь-якому місці, де б ви не працювали, у тому числі й удома. Вам може здатися, що ризик порушення конфіденційності нижчий, коли ви працюєте з дому, але насправді цей ризик підвищується, і слід бути особливо уважним, щоб зберегти конфіденційність під час роботи у віддалених місцях, у тому числі вдома.

У багатьох юрисдикціях діють спеціальні закони та нормативні акти, які стосуються дотримання конфіденційності інформації та захисту даних. Слід знати та дотримуватись законів і нормативних актів, що є застосовними до вас і роботи, яку ви виконуєте

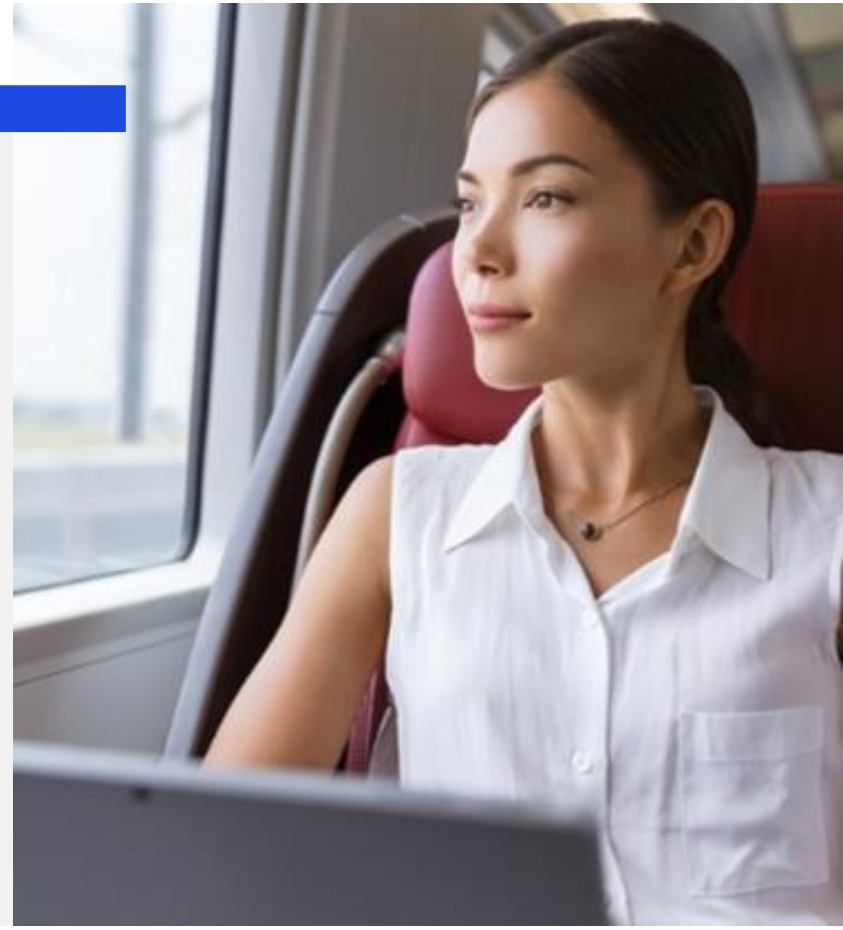
Якщо ви вважаєте, що конфіденційну інформацію та/або обладнання, що використовується для зберігання такої інформації, втрачено, викрадено або іншим чином скомпрометовано, негайно повідомте про це відповідно до встановлених процедур.

Докладніше див. у 5.3. Конфіденційність та особиста інформація .

Захист конфіденційної інформації

Незалежно від того, де ви працюєте – вдома, в офісі KPMG або в офісі клієнта – вивчіть деякі поради щодо забезпечення безпеки та захисту конфіденційної інформації та технологічних ресурсів KPMG**.** *Докладніше див. також у Глобальній політиці прийнятного використання KPMG.*

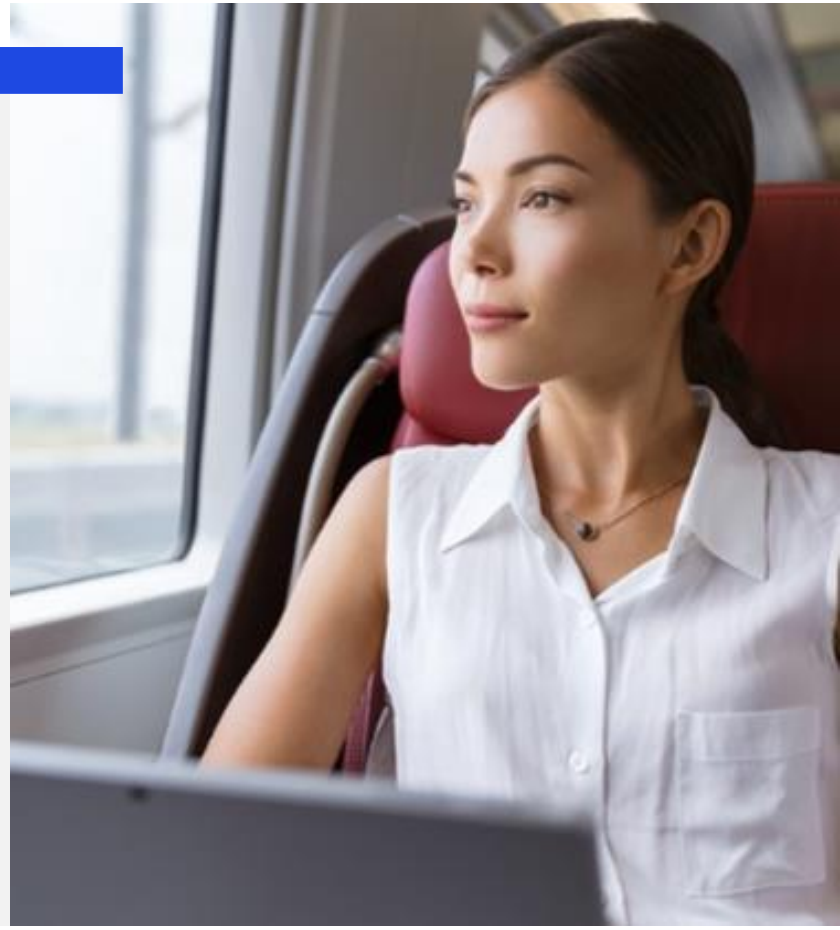
- Конфіденційна інформація повинна зберігатися тільки за допомогою технологічного рішення, затвердженого KPMG.
- Завжди зачиняйте або зберігайте в безпечному місці портативні пристрої, включаючи ноутбуки, телефони і USB-накопичувачі, в тому числі під час поїздок.
- Використовуйте захищений паролем зберігач екрана на ноутбуці і блокуйте екран ноутбука, коли ви залишаєте своє робоче місце.
- Ніколи не повідомляйте нікому свій пароль або інші облікові дані.
- Збирайте та використовуйте тільки необхідну інформацію. Повертайте або належним чином знищуйте її, як тільки у ній більше немає потреби (відповідно до нашої політики зберігання документів).
- Ніколи не залишайте конфіденційні документи без нагляду на вашому столі, принтері чи де-небудь іще.



Захист конфіденційної інформації

Незалежно від того, де ви працюєте – вдома, в офісі KPMG або в офісі клієнта – вивчіть деякі поради щодо забезпечення безпеки та захисту конфіденційної інформації та технологічних ресурсів KPMG**.** *Докладніше див. також у Глобальній політиці прийнятного використання KPMG.*

- Використовуйте тільки затверджені KPMG, захищені та зашифровані пристрої зберігання даних і тільки схвалене KPMG програмне забезпечення та застосунки.
- При відправці повідомлень електронною поштою, особливо тих, що адресовані групі осіб, запитайте себе: «Чи дійсно вони всі повинні це знати?».
- Будьте уважні та вибирайте правильних адресатів при відправці електронної пошти.
- Перед відкриттям вкладень або переходом за посиланнями в електронних листах, будь ласка, ретельно обмірковуйте ці дії..
- Будьте обережні, коли ведете бесіди в громадських місцях, вдома та під час подорожей.
- Під час конфіденційних розмов по телефону, через застосунки Skype, Microsoft Teams або з використанням інших електронних засобів використовуйте переговорну кімнату чи інше закрите місце.



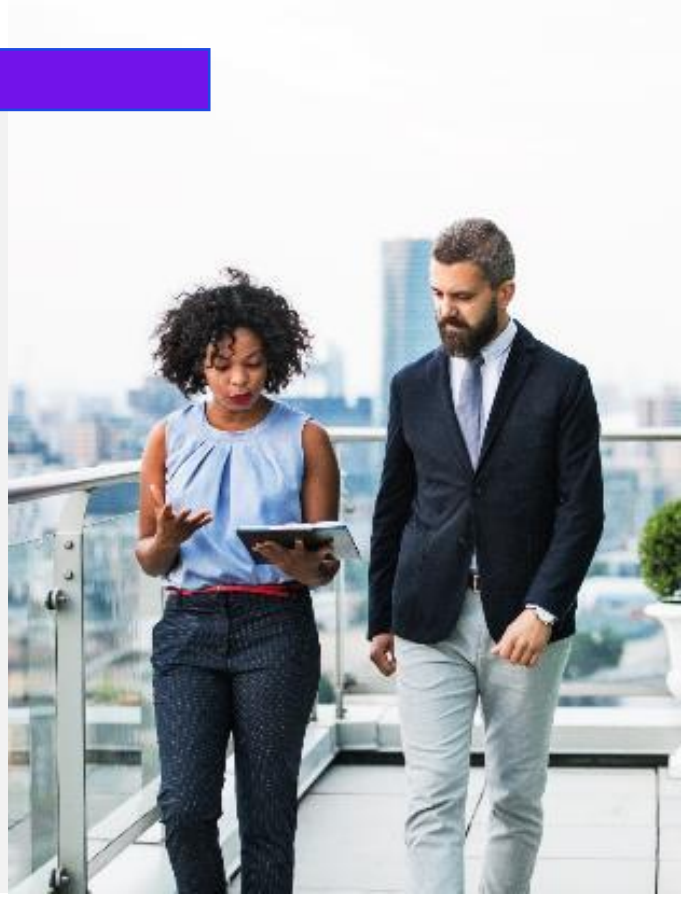
Інсайдерська торгівля

Під час роботи в KPMG, незалежно від вашої посади, вам може стати відомою закрита інформація, що стосується певної компанії або її цінних паперів. Така інформація зветься **інсайдерською інформацією**.

Торгівля акціями або іншими цінними паперами публічної компанії на основі суттєвої, непублічної інформації відома як інсайдерська торгівля.

Участь в інсайдерській торгівлі суперечить політиці KPMG. У багатьох країнах діють спеціальні закони, які забороняють інсайдерську торгівлю, а в інших країнах покарання за такого роду дії може бути передбачене кримінальним та/або цивільним законодавством

Будь-який представник KPMG, який порушує нашу політику щодо інсайдерської торгівлі, може бути підданий серйозним дисциплінарним стягненням аж до припинення співпраці/ трудових відносин. Будь-який представник KPMG, який порушує законодавство про інсайдерську торгівлю, також може бути притягнений до кримінальної відповідальності.



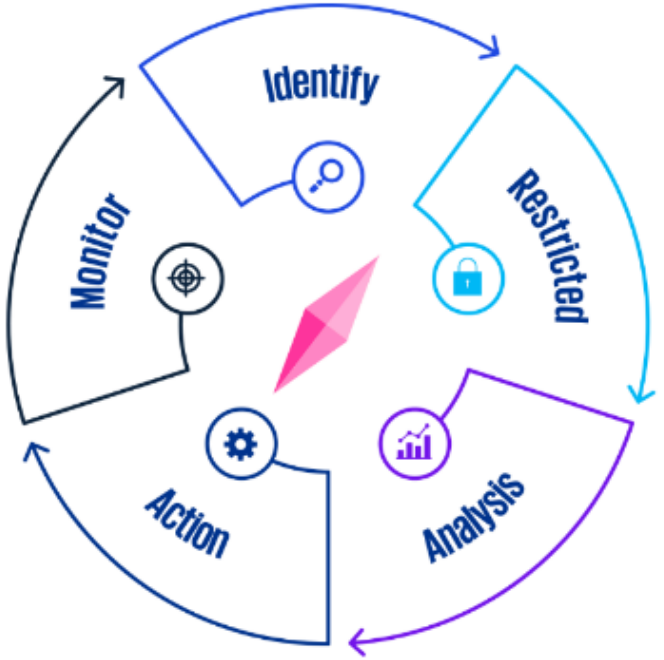
Докладніше див. у 5.6.5 Інсайдерська торгівля.

Незалежність

Незалежність складається з двох частин: незалежності мислення і незалежності поведінки:

Незалежність мислення означає, що інтереси та відносини з нашими клієнтами з аудиту та надання впевненості не загрожують нашій чесності, об'єктивності та професійному скептицизму при виконанні нашої роботи.

Незалежність поведінки означає, що наша чесність, об'єктивність та професійний скептицизм не викликають сумнівів у сторонніх осіб.



Питання незалежності можуть бути складними, тому KPMG надала низку ресурсів, які допоможуть вам орієнтуватися в ситуації, коли ви не можете визначити, яких кроків слід вжити для дотримання законів, нормативних актів та політик фірми, що є застосовними до вас.

Можливо, ви знайомі з інструментом «Цикл усвідомлення незалежності (Independence Awareness Cycle). Натисніть тут , щоб освіжити його в пам’яті.

Вимоги до повідомлення про недотримання законів і нормативних актів

У KPMG давно існують вимоги, викладені в Глобальному посібнику з управління якістю та ризиками (GQ&RMM), щодо повідомлення про потенційно незаконні дії. Кодекс етики РМСЕБ також містить положення про недотримання клієнтами (та третіми особами, що діють під їхнім керівництвом) законів і нормативних актів, які впливають на весь персонал, а не лише на працівників відділу аудиту.

Це стосується всіх законів і нормативних актів, а не лише тих, з якими ви, можливо, очікуєте зіткнутися в професійному контексті.

- Якщо ви зіткнулися з ситуацією, в якій, на вашу думку, клієнт або третя сторона не дотрималася або могла не дотриматися закону або нормативного акту, ви повинні повідомити про це партнера із завдання.
- Партнер із завдання, в свою чергу, залежно від фактів та обставин, зобов'язаний повідомити про це іншим особам.

Натисніть на кожне з полів нижче, щоб дізнатися більше.

Недотримання з боку клієнтів чи третіх сторін

Процес повідомлення

Що це означає для вас?

Недотримання з боку клієнтів чи третіх сторін

Натисніть тут, щоб повернутися до першого слайду по темі «Вимоги до повідомлення»

Політика 5.6.2 Повідомлення про порушення з боку клієнтів або третіх сторін встановлює вимоги до персоналу KPMG щодо повідомлення про підозрювані або виявлені випадки недотримання законів або нормативних актів.

Вона також включає додаткові вимоги до партнера із завдання щодо звітування про певні питання перед RMP.

Майте на увазі, що від вас так само, як і від KPMG може вимагатися, згідно з чинним законодавством або нормативними актами, повідомляти про підозри в недотриманні законів або нормативних актів у конкретний спосіб конкретній особі.

Процес повідомлення

Натисніть тут, щоб повернутися до першого слайду по темі «Вимоги до повідомлення»

Ваша фірма-член мережі KPMG зобов'язана встановити і підтримувати процес повідомлення про підозру в порушенні законів і нормативних актів, політик KPMG або професійних стандартів клієнтами, третіми особами або персоналом KPMG:

Усередині фірми-члена мережі KPMG.

- Клієнтам відповідно до вимог чинного законодавства, нормативних актів або стандартів, у т.ч., без обмежень, про будь-які порушення застосовних положень про незалежність.
- Зовнішнім сторонам (наприклад, регуляторним органам) відповідно до вимог місцевого законодавства, нормативних актів або професійних стандартів.

Що це означає для вас?

Натисніть тут, щоб повернутися до першого слайду по темі «Вимоги до повідомлення»

У всіх випадках - незалежно від того, чи є ви професіоналом у сфері аудиту, оподаткування або консультування - не мовчіть і повідомляйте про підозрювані або фактичні факти недотримання вимог вашому партнеру із завдання.

Якщо ви є партнером із завдання, вам потрібно:

- Розуміти факти та обставини виявленого або підозрюваного недотримання законів чи нормативних актів.
- Повідомляти про це RMP вашої фірми (за винятком випадків, коли питання є явно незначущим).
- Уникати попередження клієнта або третіх осіб, якщо ви підозрюєте їх у порушеннях.

RMP та внутрішній юрист KPMG визначать відповідні подальші кроки.

Якщо ви не впевнені в тому, чи порушує клієнт або третя сторона певний закон або нормативний акт, або якщо питання є явно незначущим, завжди повідомляйте про це своєму партнеру із завдання, який може повідомити про це RMP у разі необхідності..

Глобальні основи захисту інформації та конфіденційності даних. Навчальний курс, ФР 24

Вступ до курсу

Цей курс дасть вам фундаментальні знання та ключові навички поведінки, необхідні для захисту інформації наших клієнтів, інформації KPMG та нашої репутації.

Цей курс складається з 8 модулів, на проходження кожного з яких потрібно приблизно 10 хвилин:

Ви повинні переконатися, що ви ознайомлені з Політикою KPMG з питань захисту інформації та конфіденційності даних додатково до проходження цього курсу (отримайте доступ до політик вашої фірми-члена через портал вашої фірми-члена або звернувшись до місцевого підрозділу забезпечення якості та управління ризиками), якщо ви маєте акаунт KPMG

Ласкаво просимо на курс «Глобальні основи захисту інформації та конфіденційності даних».

Ми всі повинні вживати заходів для захисту інформації, пристроїв і робочого простору - вдома, в офісі чи в дорозі - щоб запобігти порушенням, які можуть мати значний вплив на бізнес і на нас особисто. Негативні наслідки можуть включати таке:

- репутаційна шкода
- порушення бізнес-процесів
- втрата суспільної довіри до нашої фірми
- санкції або штрафи з боку наших регуляторів
- можливі дисциплінарні стягнення проти окремих осіб

Ласкаво просимо на курс «Глобальні основи захисту інформації та конфіденційності даних».

Правильне розуміння цього питання є ключовим компонентом нашої стратегії, спрямованої на те, щоб стати фірмою, якій найбільше довіряють наші клієнти та громадськість.

Ми хочемо допомогти вам приймати обґрунтовані рішення та діяти правильно, коли йдеться про захист інформації та конфіденційності, і цей курс надасть вам фундаментальні знання та ключові моделі поведінки, необхідні для цього.

Пам'ятайте - де б ви не були, з ким би ви не були, що б ви не говорили, що б ви не відчували, що б ви не робили….
… Будьте в кібербезпеці в KPMG - від цього залежить наша репутація

Якщо ви вважаєте, що конфіденційна інформація й/або обладнання, яке використовується для зберігання такої інформації, було втрачено, вкрадено або іншим чином піддано компрометації, негайно повідомте про це відповідно до процедур фірми KPMG.

Сценарій 1 - Безпечна робота з інформацією

Сценарій 1 - Безпечна робота з інформацією

Нія працює над проєктом для страхової компанії. Вона розробляє додаток, який аналізуватиме обробку страхових виплат. Клієнт щойно надав набір даних для аналізу. Нія знає, що їй потрібно застосувати рівень секретності до набору даних, але вона не впевнена, який саме рівень застосувати, і як це зробити. У неї скоро спливає термін здачі роботи, тому вона не має часу, щоб розібратися з цим питанням.
Чи повинна Нія витратити час на пошук деталей класифікації зараз, або залишити це на інший час, коли вона буде менш зайнята?

Сценарій 1 - Безпечна робота з інформацією

Чи варто Нії витрачати час на пошук деталей конфіденційності зараз або відкласти його на інший час, коли вона буде менш зайнята?

Ні - вона може залишити це, оскільки її термін є важливішим, а з'ясування правильного рівня може зайняти надто багато часу

В. Так - вона повинна витратити час, щоб з'ясувати правильний рівень. Вона може звернутися до володільця інформації (як правило, до Керівника проєкту), або перевірити чи існує План захисту інформації для проєкту.

Сценарій 1 - Безпечна робота з інформацією

Чи варто Нії витрачати час на пошук деталей конфіденційності зараз або відкласти його на інший час, коли вона буде менш зайнята?

Ні - вона може залишити це, оскільки її термін є важливішим, а з'ясування правильного рівня може зайняти надто багато часу

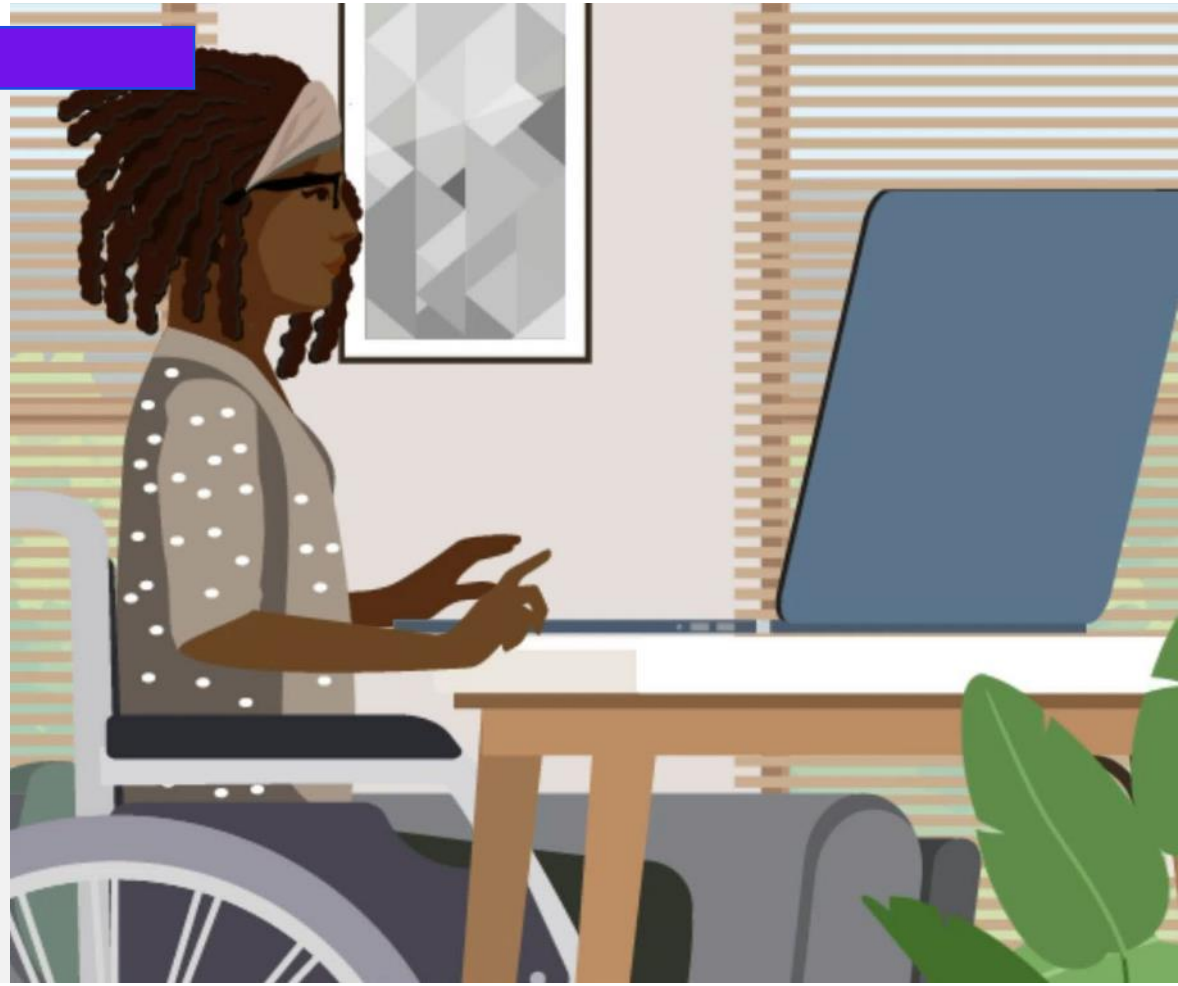
В. Так - вона повинна витратити час, щоб з'ясувати правильний рівень. Вона може звернутися до володільця інформації (як правило, до Керівника проєкту), або перевірити чи існує План захисту інформації для проєкту.

Сценарій 1 - Безпечна робота з інформацією

Вона повинна витратити час, щоб з'ясувати, яким має бути правильний рівень. Вона може звернутися до володільця інформації (як правило, до Керівника проєкту) або перевірити чи існує План захисту інформації для проєкту.

KPMG може зазнати репутаційних ризиків, втратити відносини з клієнтами та їх довіру, а також отримати штрафи від регуляторних органів, якщо інформація буде розголошена в результаті неправильної класифікації. Якщо ви не впевнені, завжди краще перевірити, аніж припускати. Занадто ризиковано помилитися в цьому відношенні.

Володілець інформації KPMG відповідає за безпечне збереження, транспортування та зберігання інформації, створеної або отриманої в KPMG, щоб знати, який рівень конфіденційності необхідно застосувати. Крім того, якщо існує План захисту інформації, в ньому будуть задокументовані процедури, необхідні для належної обробки всієї інформації та даних про проєкт.



Сценарій 1 - Безпечна робота з інформацією

Нія знає, що оскільки цей документ містить конфіденційні персональні дані, з ним потрібно завжди поводитися з максимальною обережністю. Якщо його не засекретити належним чином, він може зберігатися в неналежному місці або потрапити до рук сторонніх осіб.
У неї дуже мало часу, але за кілька хвилин їй вдається знайти потрібну інформацію на порталі. Вона застосовує найвищий рівень класифікації - KPMG Highly Confidential.
Пізніше Нія працює над звітом для клієнта. Їй потрібно десь зберегти документ - але де це зробити найкраще?

Сценарій 1 - Безпечна робота з інформацією

Де Нія має зберегти документ?

А.Їй слід дізнатися у своєї команди, яке сховище вони використовують для зберігання всієї проєктної документації. Або вона може перевірити, чи існують якісь особливі вимоги щодо безпеки зберігання документів для цього проєкту. Такі вимоги можуть бути викладені в Плані захисту інформації з урахуванням вимог клієнта та типу інформації, що обробляється.

В. Буде зручніше, якщо вона збереже його на своєму робочому столі, оскільки це забезпечує легкий доступ. Він їй скоро знадобиться, тому вона повинна мати можливість швидко його знайти. Крім того, на ноутбуках KPMG постійно оновлюються функції безпеки, тому вони не знаходяться під ризиком.

Сценарій 1 - Безпечна робота з інформацією

Де Нія має зберегти документ?

А.Їй слід дізнатися у своєї команди, яке сховище вони використовують для зберігання всієї проєктної документації. Або вона може перевірити, чи існують якісь особливі вимоги щодо безпеки зберігання документів для цього проєкту. Такі вимоги можуть бути викладені в Плані захисту інформації з урахуванням вимог клієнта та типу інформації, що обробляється.

В. Буде зручніше, якщо вона збереже його на своєму робочому столі, оскільки це забезпечує легкий доступ. Він їй скоро знадобиться, тому вона повинна мати можливість швидко його знайти. Крім того, на ноутбуках KPMG постійно оновлюються функції безпеки, тому вони не знаходяться під ризиком.

Сценарій 1 - Безпечна робота з інформацією

Її робоча група, швидше за все, використовує внутрішню систему документообігу, оскільки вона є найбільш безпечною. Не рекомендується зберігати інформацію на робочому столі, особливо конфіденційну, оскільки вона знаходиться під більшим ризиком втрати або крадіжки. Краще зберігати її в захищеному сховищі, сертифікованому KPMG, оскільки це запобігає несанкціонованому доступу.

Вам не слід зберігати конфіденційні персональні дані або інформацію з високим ступенем конфіденційності в програмі Teams, якщо тільки це не було схвалено Керівником проєкту. Вам ніколи не слід зберігати інформацію KPMG або клієнтів у зовнішньому хмарному рішенні, такому як Dropbox, якщо це не було схвалено клієнтом та Національним спеціалістом з питань IT-безпеки (NITSO).

Сценарій 1 - Безпечна робота з інформацією

Нія розуміє, що документ слід зберігати в безпечному місці, і це, ймовірно, передбачено умовами договору з клієнтом. Менеджер проєкту повинен знати більше. Вона пише своєму менеджеру повідомлення, щоб дізнатися, яке сховище команда використовує для цього проєкту. Група по проєкту використовує Teams для цього проєкту, тому вона зберігає документ там. Після цього її менеджер відповідає, що він хотів б, щоб Нія надала доступ іншим членам команди проєкту, яким може знадобитися попрацювати з даними пізніше. Нія вагається, чи правильно це, адже вона не хотіла б, щоб хтось отримав доступ до конфіденційної інформації про неї саму, якщо це не буде йому потрібно для роботи. Чи слід їй надати доступ всім членам команди?

Сценарій 1 - Безпечна робота з інформацією

Чи повинна Нія надати доступ цим колегам?

A.Тільки після консультації зі своїм менеджером. Документ містить конфіденційну інформацію, тому доступ до нього повинен бути обмежений лише тими, кому це необхідно знати або використовувати для виконання службових обов'язків.

A.Так - вона повинна зробити те, що просить менеджер, не ставлячи під сумнів його вказівки. Менеджер усвідомлює ризики надання доступу надто великій кількості людей без потреби.

Сценарій 1 - Безпечна робота з інформацією

Чи повинна Нія надати доступ цим колегам?

A.Тільки після консультації зі своїм менеджером. Документ містить конфіденційну інформацію, тому доступ до нього повинен бути обмежений лише тими, кому це необхідно знати або використовувати для виконання службових обов'язків.

A.Так - вона повинна зробити те, що просить менеджер, не ставлячи під сумнів його вказівки. Менеджер усвідомлює ризики надання доступу надто великій кількості людей без потреби.

Сценарій 1 - Безпечна робота з інформацією

Якщо вам здається, що щось виглядає неправильно, завжди потрібно перевіряти. Вірогідно, що менеджер може бути не в курсі всіх обставин або не повністю зважив ризики, пов'язані з наданням доступу цим колегам.

Обережність ніколи не буває зайвою, і ваш менеджер вважатиме за краще, якщо ви повідомите про проблеми з безпекою, а не мовчатимете, що може призвести до серйозного витоку даних з серйозними наслідками для KPMG.

Сценарій 1 - Безпечна робота з інформацією

Нія знову надсилає повідомлення своєму менеджеру, пропонуючи обмежити доступ до звіту лише особами, яким він необхідний для роботи. Керівник погоджується і дякує Нії за те, що вона подбала про безпеку. Нія надає доступ лише тим членам команди, яким потрібно працювати з даними.

Сценарій 1 - Безпечна робота з інформацією

В цьому сценарії ви ознайомилися з прикладами застосування правильного рівня конфіденційності, безпечного зберігання конфіденційних даних та безпечних прав доступу.

Існують важливі моменти, які слід враховувати при безпечному поводженні з інформацією.

Щоб дізнатися більше, прочитайте наступні КЛЮЧОВІ РЕКОМЕНДАЦІЇ.

Захист інформації від несанкціонованого доступу –

KPMG має 3 рівні Захисту інформації від несанкціонованого доступу:

KPMG Публічний документ

Це стосується інформації, **яка є загальнодоступною** і може бути розкрита без шкоди для клієнта або KPMG. Приклади:

- Інформація на зовнішніх веб-сайтах KPMG
- Прес-релізи
- Маркетингові матеріали
- Опубліковані річні звіти

KPMG Confidential

Це **класифікація за замовчуванням**, яка застосовується до інформації, несанкціоноване розкриття, компрометація або знищення якої прямо чи опосередковано може мати негативний вплив на KPMG, її клієнтів або співробітників.
Приклади:

- Документація, що стосується переважно проєктів
- Персональні дані
- Внутрішня інформація, що включає регламенти, кадрову та фінансову звітність
- Інформація про загальногосподарські адміністративні витрати

KPMG Highly Confidential

Це стосується інформації, розголошення якої не уповноваженим особам відкриє доступ до комерційної таємниці, поставить під загрозу інтереси KPMG або її клієнтів чи **завдасть серйозної особистої або фінансової шкоди**.
Приклади:

- Конфіденційна персональна інформація
- Конфіденційна інформація, що стосується цін та ринку
- Конфіденційна документація, що стосується проєктів
- Коли третя сторона встановлює найвищий рівень конфіденційності
- з квітня 2024 року ця категорія буде перейменована на обмежену інформацію KPMG (KPMG Restricted)

Плани захисту інформації (IPP)

Що таке План захисту інформації (IPP)?

Це інструмент, який можна використовувати для **документування заходів і процедур,** яких може вжити проєктна команда для належного захисту та обробки інформації та даних для цього проєкту. Це допомагає нам відповідати мінімальним вимогам безпеки наших клієнтів, а також гарантувати, що члени проєктної групи розуміють свої особисті обов'язки щодо захисту інформації клієнта.

Who is responsible for the IPP?

Керівник проєкту (як володілець інформації) повинен скласти, підтримувати та управляти Планом захисту інформації. Однак це завдання можна доручити іншому члену проєктної групи, який добре розуміється на взаємодії з клієнтом та обробці інформації про нього.

Партнер по проєкту повинен нести відповідальність за затвердження заповненого Плану захисту інформації, оскільки він має необхідний досвід і повноваження.

Всі **члени проєктної групи** (включаючи підрядників) будуть зобов'язані дотримуватися положень Плану захисту інформації.

Де я можу знайти типовий шаблон Плану захисту інформації?

Типовий шаблон Плану захисту інформації міститься у Розділі **15.3.3 Посібника з контролю якості та управління ризиками KPMG (GQRMM)**.

Утримання, зберігання та утилізація

Важливо захищати документи та інформацію клієнтів (інформацію KPMG або інформацію, пов'язану із проєктами, отриману в ході надання професійних послуг клієнту)) від **втрати, знищення, фальсифікації, несанкціонованого доступу та несанкціонованого розголошення** відповідно до законодавчих, регуляторних, договірних та бізнес-вимог.

Поводження з інформацією на паперових носіях

Захищайте інформацію на паперових носіях, наприклад, на паперових **копіях, роздруківках, друкованих матеріалах, у файлах або документах** , незалежно від того, чи працюєте ви в офісі KPMG, у клієнта або у віддаленому місці:

- Завжди безпечно зберігайте конфіденційні файли KPMG та клієнтів **у захищених, спеціально відведених для цього місцях**, або у затверджених KPMG постачальників послуг із зберігання даних за межами офісу (і постійно оновлюйте відповідні інвентаризаційні відомості).
- Повертайте інформацію на паперових носіях у **безпечне місце зберігання,** як тільки завершите будь-які огляди або довідкову роботу.
- Якщо вам потрібно буде **безпечно надіслати конфіденційні документи поштою**, дотримуйтеся процедури, прийнятої у вашій Фірмі-члені (наприклад, скористайтеся послугами уповноваженої місцевої кур'єрської служби).

Зберігання

Зберігайте документи протягом належного періоду часу відповідно до **Графіку зберігання документів вашої Фірми-члена**. Якщо документи не потрібно зберігати, видаліть їх або безпечно утилізуйте відповідно до політик і процедур вашої Фірми-члена.

Цифрове сховище

- Зберігайте записи в **затвердженій системі документообігу,** що використовується вашою Фірмою-членом (завжди перевіряйте та отримуйте дозвіл перед зберіганням будь-яких матеріалів з високим ступенем конфіденційності).
- Не створюйте резервні копії пристроїв KPMG (і даних, що **зберігаються на них) у несанкціонованих хмарних сервісах**.

Утилізація

Утилізуйте документи, пристрої та цифрові файли згідно з політикою та процедурами вашої Фірми-членa:

Паперові документи

- Утилізуйте матеріали в офісі в **конфіденційному сміттєвому контейнері**
- Утилізуйте матеріали вдома, використовуючи **перехресний шредер** (за умови, що він відповідає стандарту безпеки DIN 66399, рівень 4 або вище)

Devices

- Наприклад, непотрібні ноутбуки, USB-накопичувачі, мобільні пристрої, жорсткі диски
- Надсилайте або передавайте їх до підрозділу інформаційної безпеки **(ITS)**, який надійно утилізує їх для вас

Emails/ digital files

- Спочатку перевірте **Політику зберігання даних вашої Фірми-члена,** щоб переконатися, що їх не потрібно зберігати довше
- **Видаляйте вручну** файли та електронні листи, які більше не потрібні

Права доступу та необхідна службова інформація

Коли вам довіряють конфіденційну або персональну інформацію, ви несете відповідальність за те, **щоб забезпечити доступ до неї лише тим, кому вона необхідна для роботи**, і хто має відповідний дозвіл на доступ до неї. Лише той факт, що хтось працює в KPMG, не обов'язково означає, що йому потрібен доступ до персональної та конфіденційної інформації.

Для захисту конфіденційності та кращого розуміння того, якою інформацією ділитися (і з ким):

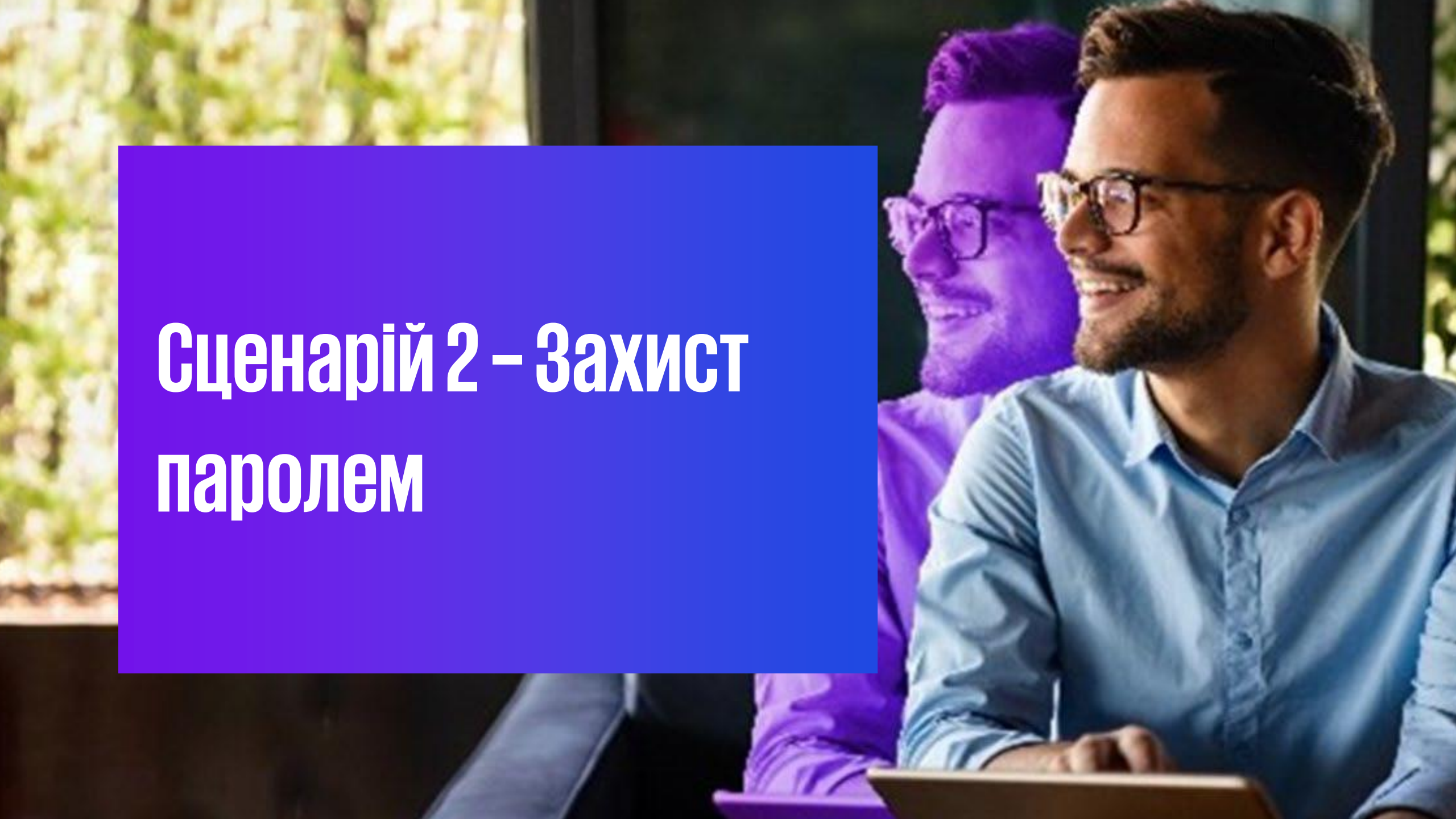
Не згадуйте та не описуйте деталі, за якими можна ідентифікувати конкретного клієнта

Будьте уважні до того, з ким ви ділитеся або обговорюєте персональну або конфіденційну інформацію, навіть у межах KPMG

Обмежте доступ до інформації лише тими людьми, які мають на це право, і переконайтеся, що ви маєте доступ лише до тієї інформації, яку ви уповноважені бачити

Переконайтеся, що розкриття інформації відповідає очікуванням клієнта та умовам відповідного завдання

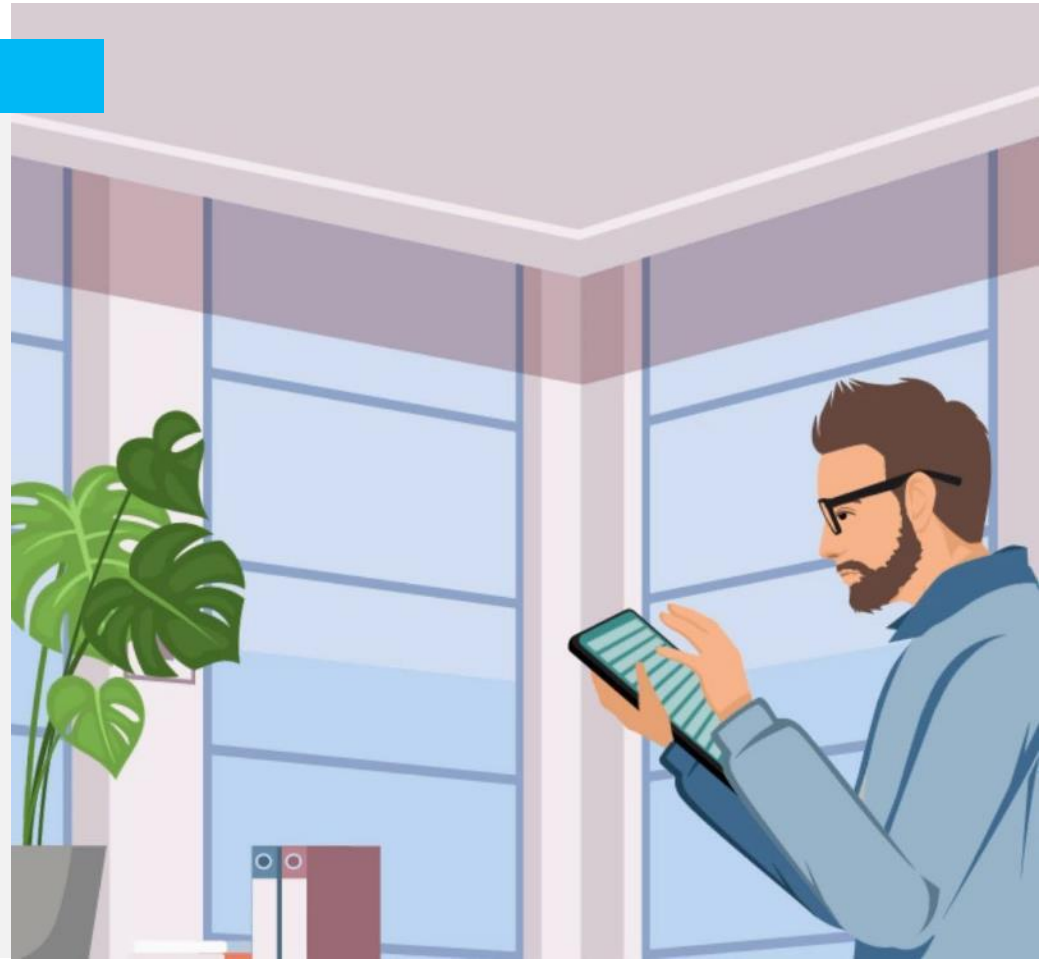
Переконайтеся, що треті сторони та постачальники мають законну потребу та належний дозвіл на доступ до персональної та конфіденційної інформації



Сценарій 2 – Захист паролем

Сценарій 2 – Захист паролем

Алекс щойно приєднався до KPMG. Йому потрібно встановити пароль до свого нового облікового запису. Він згадує свій вступний інструктаж, де обговорювалися вимоги до паролів. Йому важко придумати пароль, але він розуміє, що його особистий пароль від Hotmail відповідає вимогам. Він на мить замислюється, чи варто це робити. Чи повинен Алекс повторно використовувати свій особистий пароль для входу в обліковий запис KPMG?



Сценарій 2 – Захист паролем

Чи варто Алексу повторно використовувати свій особистий пароль для входу до системи KPMG?

A. Так, можна повторно використовувати особистий пароль, якщо він відповідає вимогам KPMG щодо довжини та надійності.

B. Ні, ви ніколи не повинні застосовувати той самий пароль для входу в KPMG, який ви використовуєте для особистих облікових записів.

Сценарій 2 – Захист паролем

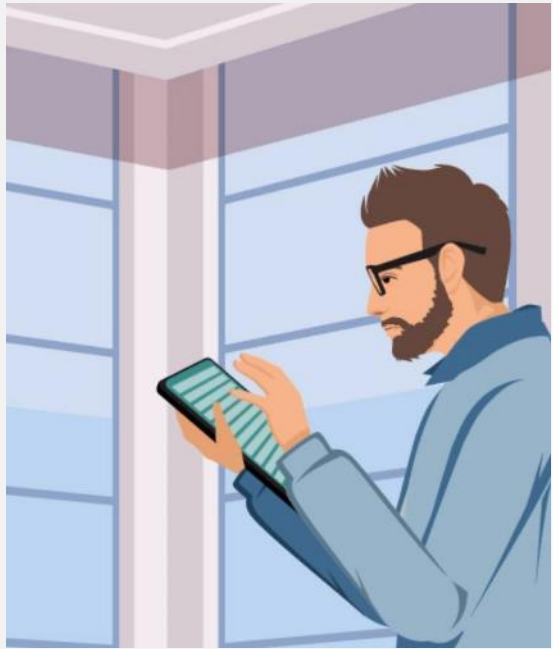
Чи варто Алексу повторно використовувати свій особистий пароль для входу до системи KPMG?

A. Так, можна повторно використовувати особистий пароль, якщо він відповідає вимогам KPMG щодо довжини та надійності.

B. Ні, ви ніколи не повинні застосовувати той самий пароль для входу в KPMG, який ви використовуєте для особистих облікових записів.

Сценарій 2 – Захист паролем

Ви завжди повинні використовувати унікальний пароль для своїх облікових записів KPMG. В іншому випадку, якщо хакер викраде або вгадає ваш особистий пароль, він зможе отримати доступ до мережі та систем KPMG, а також до вашого облікового запису KPMG.



Сценарій 2 – Захист паролем

Алекс пам'ятає з вступного інструктажу, що для входу в систему KPMG не можна використовувати той самий пароль, який ви використовуєте для особистих облікових записів. Якщо хакер викраде або вгадає його особистий пароль, він також отримає доступ до його облікового запису KPMG.
Він оглядає кімнату і бачить три речі, які можна використати для придумування пароля KPMG. Він придумує довгий, надійний пароль, який буде легко запам'ятати.

Сценарій 2 – Захист паролем

Надійні паролі мусять:

- Містити мінімум 8 символів
- Використовувати комбінацію великих і малих літер, цифр та/або спеціальних символів
- Змінюватися щонайменше кожні 90

Бажано, щоб ваш пароль був таким, який ви зможете запам'ятати. Спробуйте придумати фразу, що складається з трьох непов'язаних слів, а потім зробіть її такою, щоб вона відповідала нашим вимогам до паролів.

Наприклад:

змінюється на:

bi£dSpoonwint%r

Сценарій 2 – Захист паролем

Пізніше Алекс розмовляє зі своїм колегою Сандживом про інструмент для очищення даних, який його команда використовує під час роботи над проєктом. Санджив раніше просив завантажити цей зручний додаток, щоб використовувати його для роботи з клієнтами, але йому було відмовлено. Він запитує Алекса, чи не поділиться той своїми обліковими даними, щоб він міг користуватися додатком з акаунта Алекса. Алекс не впевнений, чи може він поділитися своїми обліковими даними KPMG: він точно не поділиться своїми особистими даними з кимось. Як він повинен відповісти Сандживу?

Сценарій 2 – Захист паролем

Як Алекс має відповісти Сандживу?

A . Алекс слід сказати йому, що за жодних обставин не можна ділитися своїми обліковими даними для входу в систему. Це пов'язано з надто великим ризиками.

B. Йому слід поділитися своїми даними, щоб допомогти колезі з його проєктом. Це не є ризиком, оскільки вони працюють в одному відділі, а додаток був схвалений для використання.

Сценарій 2 – Захист паролем

Як Алекс має відповісти Сандживу?

A . Алекс слід сказати йому, що за жодних обставин не можна ділитися своїми обліковими даними для входу в систему. Це пов'язано з надто великим ризиками.

B. Йому слід поділитися своїми даними, щоб допомогти колезі з його проєктом. Це не є ризиком, оскільки вони працюють в одному відділі, а додаток був схвалений для використання.

Сценарій 2 – Захист паролем

Алекс відповідає за всю операційну діяльність, яка відбувається в його обліковому записі KPMG. Отже, якщо Санджив увійде в систему від імені Алекса і виконає несанкціоновані дії (наприклад, обробку даних клієнта в програмі, яка не була схвалена для використання в цьому завданні), Алекс також буде нести відповідальність за порушення контракту.

Тільки тому, що додаток схвалений для використання в рамках одного проєкту з клієнтом, він може бути не схвалений для іншого проєкту, навіть в межах одного відділу (наприклад, тому що кожен клієнт може мати унікальні вимоги до безпеки, або тому, що існує вищий ризик, якщо йдеться про більш конфіденційну інформацію).

Інші ризики включають таке:

- Санджив може отримати доступ до інформації KPMG або клієнта, яку він не має права переглядати, або до систем KPMG, до яких він не повинен мати доступу (наприклад, якщо Алекс має привілейований доступ до системи або мережі).
- Він може виконати несанкціоновані дії (наприклад, внести зміни в роботу), які будуть приписані Алексу.
- Надання спільного доступу до програмного забезпечення, наданого третіми особами, може порушувати умови ліцензійної угоди.

Сценарій 2 – Захист паролем

Алекс каже Сандживу, що не може нікому повідомляти свій пароль.
Він пояснює, що несе відповідальність за всі дії, які відбуваються в його обліковому записі KPMG, включно з будь-якими діями, які можуть призвести до витоку даних. Це занадто великий ризик. Санджив розуміє аргументи Алекса - він ще раз поговорить зі своїм менеджером проєкту про можливість використання додатку.

Сценарій 2 – Захист паролем

У цьому сценарії ми дізналися про те, як встановити надійний, унікальний пароль і не ділитися обліковими даними.

Ознайомтеся з ключовими моментами, які слід враховувати при виборі пароля, вибравши КЛЮЧОВІ МІРКУВАННЯ.

Паролі

Щоб захиститися від посягань кіберзлочинців, які прагнуть отримати доступ до мережі та систем KPMG, **важливо створювати надійні паролі** . Слабкий пароль можна вгадати дуже швидко, наприклад, пароль123 можна розгадати за лічені секунди.

Тим не менш, складний пароль (або парольну фразу), який **важко вгадати, але легко запам'ятати,** можна зламати за кілька місяців або більше, а до того часу пароль на вашому пристрої KPMG буде змінено згідно з політикою.

Надійний пароль

footBallMonkey2shaDow@

roCket%time8gasolinE

Tomato&holidaY29parent

jIgsaW73quicKly$kNife

Слабкий пароль

password123

IloveUnited

Summer2023

P@$$w0rd

Це мінімальні вимоги до паролів (але перевірте політику вашої Фірми-члена, оскільки вона може мати більш суворі вимоги):

A) **Мінімальна довжина пароля**	Паролі повинні містити щонайменше 8 символів.
B) **Складність пароля**	Паролі повинні включати будь-які три з наступних чотирьох ознак: Великі літери, малі літери, алфавітно-цифрові символи та спеціальні символи (наприклад, #*&% тощо).
C) **Період зміни паролю**	Паролі повинні замінюватися щонайменше кожні 90 днів

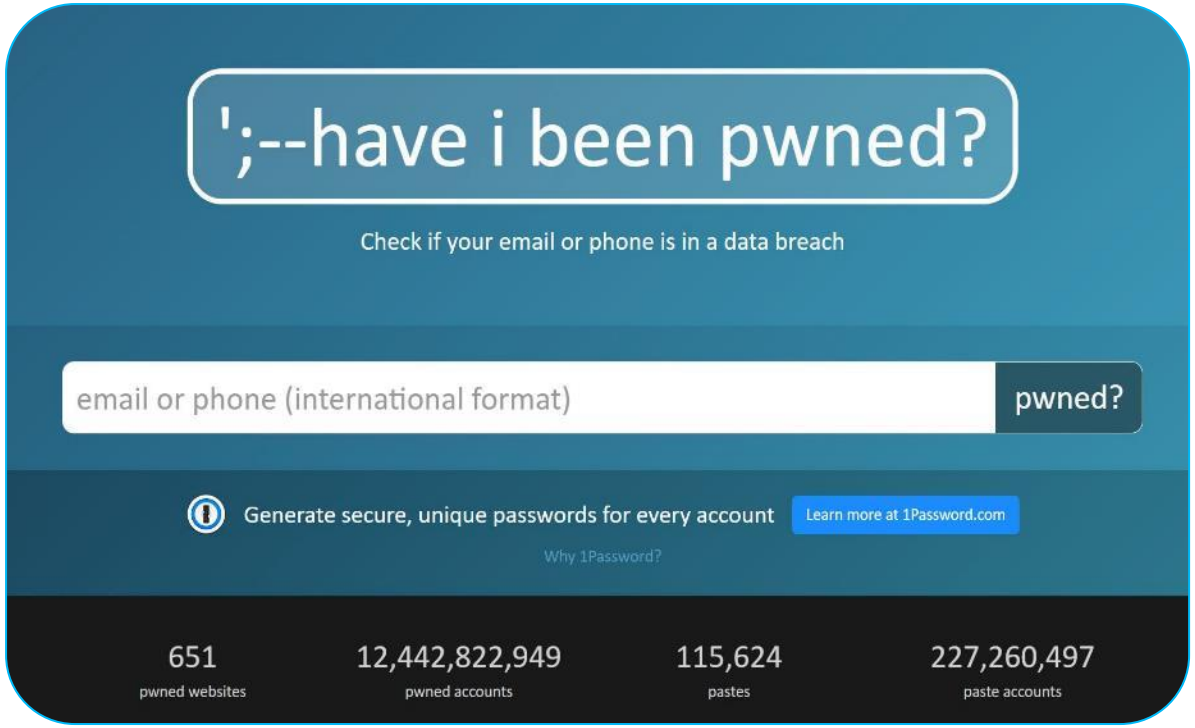
Щоб зробити свій пароль легким для запам'ятовування, радимо використовувати 3 випадкових слова (наприклад, swipe, house, paper) і вставляти спеціальні символи та цифри: **sWipe4house%paper**

Уникайте таких загальновживаних слів, як **"p@55word"** чи **""** і уникайте загальних фраз на кшталт **"IloveMyDog“,** або слів, що асоціюються з вами, які можна легко вгадати, наприклад, прізвище, ім'я домашнього улюбленця, назва компанії, улюблений фільм або спортивна команда, ваше ім'я користувача

Паролі

Пам'ятайте, що ви несете відповідальність **за всі дії в системі,** які відбуваються з використанням ваших облікових даних, наданих KPMG (логін/паролі для входу в систему).

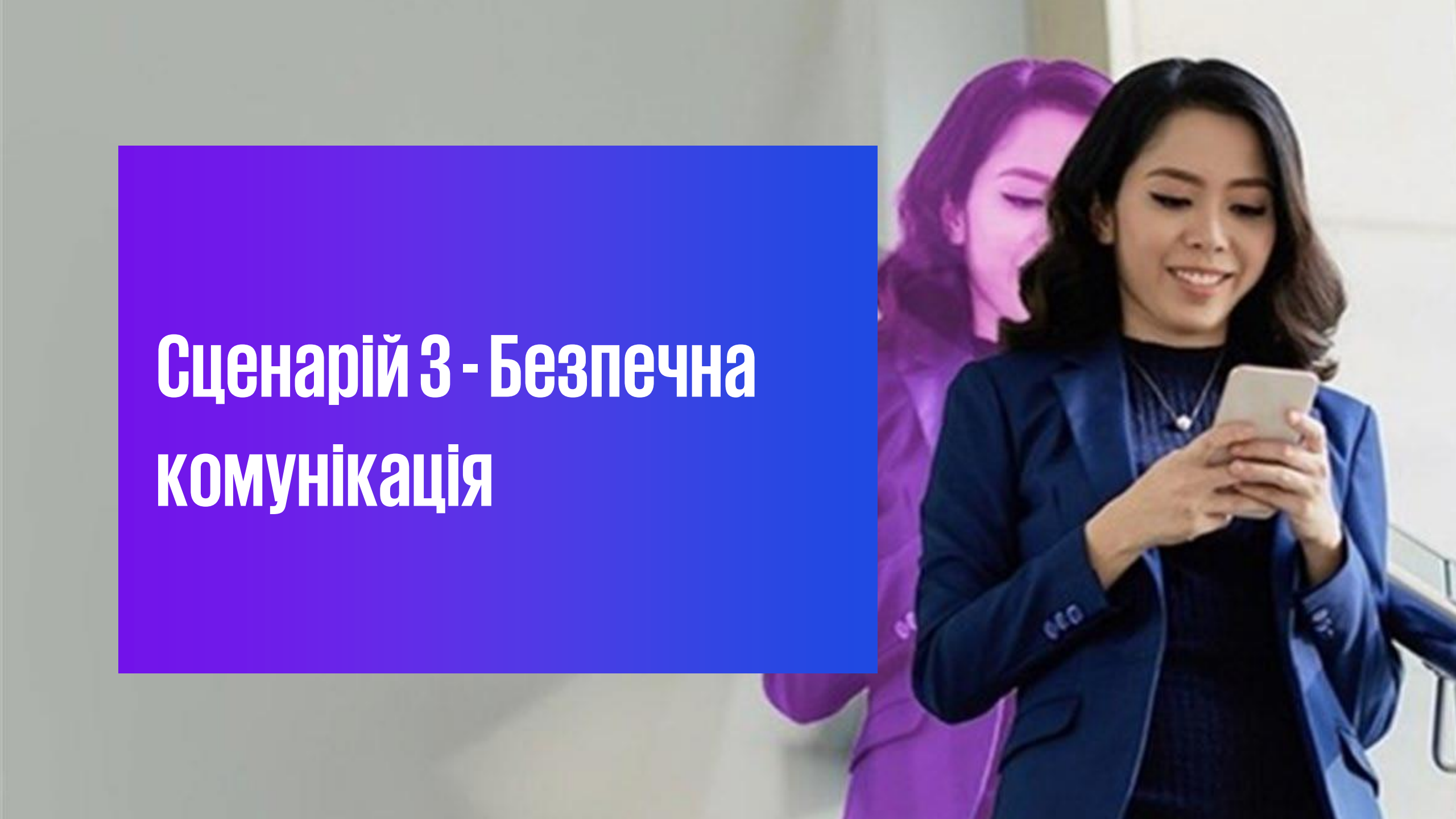
- Паролі, які ви використовуєте для систем KPMG, **повинні бути унікальними** і не повинні використовуватися для будь-яких інших (наприклад, особистих) облікових записів.
- Захищайте всі паролі, які використовуються для доступу до пристроїв KPMG – **не передавайте їх іншим особам** і не записуйте їх.
- Подбайте про те, щоб захистити всі пов'язані з ними механізми доступу **такі як PIN-коди, токени та пристрої доступу,** від втрати та розголошення.



Перевірте, чи не була ваша адреса електронної пошти - робоча або особиста - скомпрометована в результаті витоку даних, відвідавши зовнішній веб-сайт https://haveibeenpwned.com/.

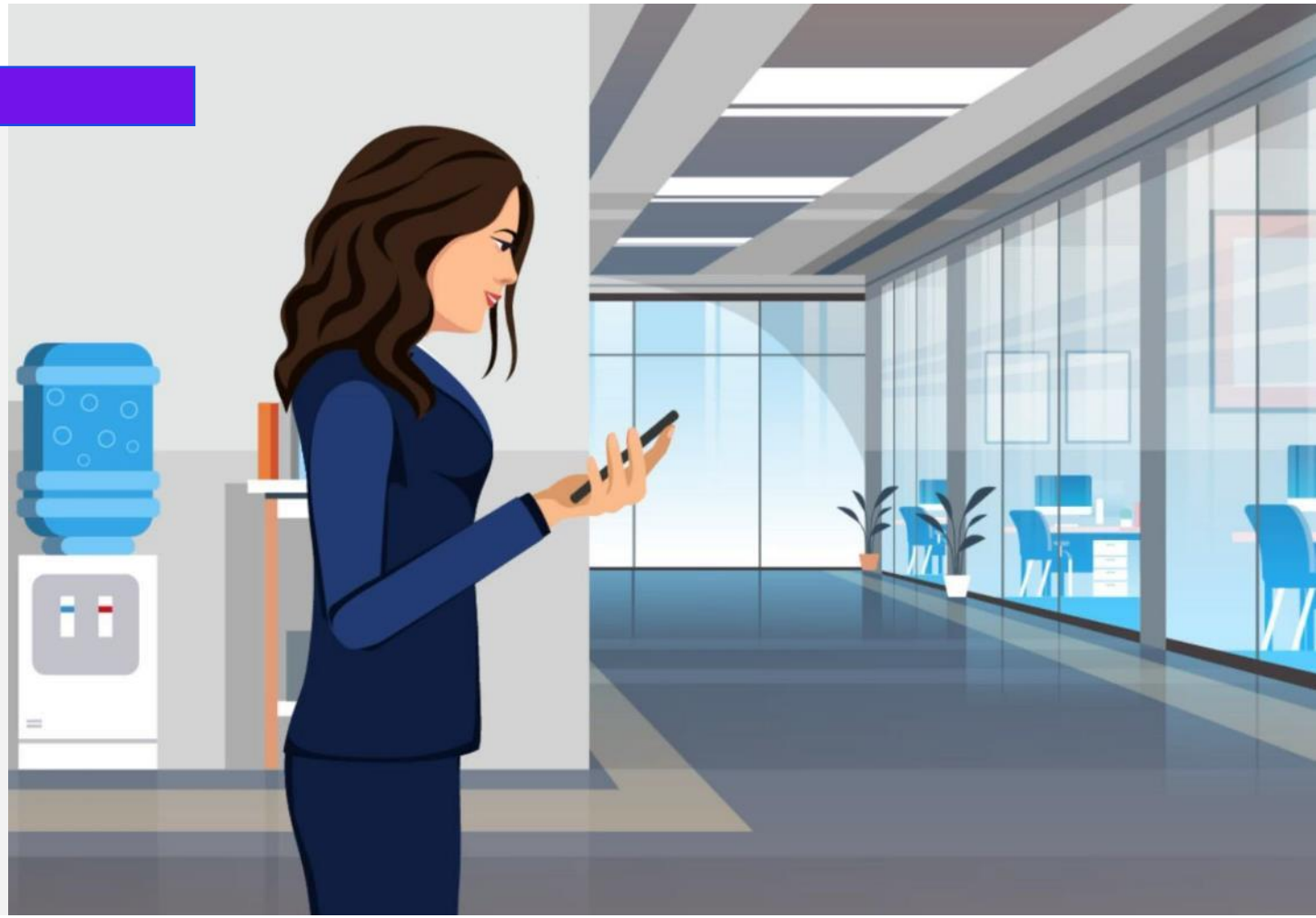
Якщо це сталося, негайно змініть пароль і зверніться до місцевої служби ITS.

Сценарій 3 - Безпечна комунікація



Сценарій 3 - Безпечна комунікація

Лі щойно прийшла в офіс, як отримала повідомлення від своєї колеги Елени. Незабаром у Елени інструктаж для менеджера проєкту, тож Лі хоче відповісти швидко.
Але вона не впевнена, чи варто обговорювати деталі роботи з клієнтом у WhatsApp. Як Лі має відповісти Елені?



Сценарій 3 - Безпечна комунікація

Як Лі повинна відповісти Елені?

A. Лі має надати їй коротку інформацію у відповідь у WhatsApp, оскільки Елені інформація потрібна якнайшвидше. Це допустимо, якщо вона не розголошує жодної конфіденційної інформації.

B. Для надсилання повідомлення Лі повинна використовувати затверджений канал зв'язку (наприклад, Exchange / Outlook, MS Teams).

Сценарій 3 - Безпечна комунікація

Як Лі повинна відповісти Елені?

A. Лі має надати їй коротку інформацію у відповідь у WhatsApp, оскільки Елені інформація потрібна якнайшвидше. Це допустимо, якщо вона не розголошує жодної конфіденційної інформації.

B. Для надсилання повідомлення Лі повинна використовувати затверджений канал зв'язку (наприклад, Exchange / Outlook, MS Teams).

Сценарій 3 - Безпечна комунікація

WhatsApp підходить для спілкування з колегами на особисті теми, але не варто використовувати цю програму для ділового спілкування (особливо при обговоренні конфіденційних клієнтських завдань), оскільки вона не схвалена KPMG для спілкування. Несанкціоновані програми можуть бути не безпечними і наражати нас на ризик витоку даних. Були навіть випадки, коли зловмисники створювали фейкові профілі під виглядом старших колег і просили розкрити конфіденційну інформацію.

Використання такої системи може також порушити стандарти зберігання даних фірми або призвести до того, що інформація перетне кордони та порушить місцеві правила конфіденційності даних.

Використання затвердженого методу може забрати більше часу, але краще убезпечити себе і допомогти запобігти потраплянню конфіденційної інформації в чужі руки.

Сценарій 3 - Безпечна комунікація

Лі розуміє, що WhatsApp не є схваленим додатком для комунікацій KPMG, тому його не можна використовувати для ділових розмов. Вона вирішує, що найкраще відповісти через Teams.

Це займе лише на кілька секунд більше часу і означатиме, що інформація буде менш схильна до ризику бути перехопленою третьою стороною.

Пізніше Лі отримує повідомлення від керівника проєкту Якоба, який просить її надіслати резюме свого звіту Маркусу в компанії клієнта. Вона друкує електронного листа клієнту.

Лі вагається - це цінна ринкова інформація, яку вона збирається відправити назовні. Вона не впевнена, чи можна включати її в основну частину листа. Як Лі має забезпечити належний захист інформації, перш ніж надсилати її клієнту?

Сценарій 3 - Безпечна комунікація

Як Лі має переконатися, що інформація захищена належним чином, перш ніж надсилати її клієнту електронною поштою?

A. Лі потрібно вжити додаткових заходів і зашифрувати конфіденційну інформацію за допомогою затвердженого інструмента (наприклад, WinZip), перш ніж додавати її до електронного листа.

B. Лі може відправити інформацію в тексті електронного листа, якщо він надсилається за допомогою затвердженого KPMG інструменту електронної пошти (наприклад, програми Outlook).

Сценарій 3 - Безпечна комунікація

Як Лі має переконатися, що інформація захищена належним чином, перш ніж надсилати її клієнту електронною поштою?

A. Лі потрібно вжити додаткових заходів і зашифрувати конфіденційну інформацію за допомогою затвердженого інструмента (наприклад, WinZip), перш ніж додавати її до електронного листа.

B. Лі може відправити інформацію в тексті електронного листа, якщо він надсилається за допомогою затвердженого KPMG інструменту електронної пошти (наприклад, програми Outlook).

Сценарій 3 - Безпечна комунікація

Інформація про придбання є конфіденційною і потребує захисту при передачі стороннім особам. Якщо ви надсилаєте конфіденційну інформацію або дані у вкладених файлах клієнту або іншій третій стороні, їх потрібно зашифрувати за допомогою схваленого продукту, наприклад, WinZip. Пароль шифрування повинен бути надісланий окремим способом (наприклад, телефонним дзвінком або SMS), оскільки це мінімізує ризик перехоплення даних та отримання доступу до інформації з боку зловмисників.

Щоразу, коли ви надсилаєте конфіденційну або дуже конфіденційну інформацію клієнту, завжди спочатку перевіряйте, чи схвалив клієнт спосіб зв'язку (наприклад, електронну пошту), який ви будете використовувати. Проконсультуйтеся з Керівником або Менеджером проєкту або перевірте План інформаційної безпеки за проєктом (ПІБ), якщо такий є.

Сценарій 3 - Безпечна комунікація

Лі знає, що інформація є надто чутливою, щоб надсилати її незахищеною. Якби вона надсилала конфіденційну інформацію про себе електронною поштою, вона б хотіла максимально захистити її від несанкціонованого розголошення. Вона вирішує вставити резюме в документ Word і зашифрувати його. Тепер їй залишається лише додати ім'я Маркуса в поле адреси і натиснути кнопку "Надіслати". Вона поспішає, бо запізнюється на каву з Еленою. Лі випадково надіслала листа одному зі своїх старих клієнтів, Мартіну Доусону. Спочатку вона панікує, але потім згадує, що інформація була захищена шифруванням, а у нього немає пароля для відкриття файлу. Вона може це виправити, попросивши Мартіна видалити лист і підтвердити, коли він це зробить. Лі не впевнена, що зробила все, що потрібно в цій ситуації. Що ще їй потрібно зробити?

Сценарій 3 - Безпечна комунікація

Що ще потрібно зробити Лі?

A. Їй потрібно негайно повідомити про це як про витік даних.

B. Їй потрібно повідомити про це Керівнику проєкту під час їхньої наступної зустрічі. Про це не потрібно повідомляти як про витік даних, оскільки Мартін не мав можливості прочитати зашифровані дані, і вона вважає, що він видалив електронний лист. Це лише спричинить непотрібну тривогу і може зашкодити відносинам з клієнтом.

Сценарій 3 - Безпечна комунікація

Що ще потрібно зробити Лі?

A. Їй потрібно негайно повідомити про це як про витік даних.

B. Їй потрібно повідомити про це Керівнику проєкту під час їхньої наступної зустрічі. Про це не потрібно повідомляти як про витік даних, оскільки Мартін не мав можливості прочитати зашифровані дані, і вона вважає, що він видалив електронний лист. Це лише спричинить непотрібну тривогу і може зашкодити відносинам з клієнтом.

Сценарій 3 - Безпечна комунікація

Навіть якщо Мартін не має пароля, щоб прочитати зашифровані дані в електронному листі, Лі все одно повинна негайно повідомити про цей випадок. Після цього особа, яка проводить розслідування

Важливо негайно повідомляти про фактичні або підозрювані порушення безпеки через місцевий канал зв'язку (наприклад, IT-службу, Національного спеціаліста з питань IT-безпеки (NITSO) або Спеціаліста з питань конфіденційності (PL)), щоб вони могли швидко відреагувати та мінімізувати будь-яку шкоду для наших операцій і репутації, спричинену порушенням.

Ви не повинні інформувати будь-кого іншого, включаючи Керівника проєкту, клієнта або інших колег, не проконсультувавшись з вашим місцевим Підрозділом з управління ризиками. Якщо ви випадково надіслали електронного листа, що містить конфіденційну інформацію, на помилкову адресу, отримайте дозвіл від місцевого Підрозділу з управління ризиками зв'язатися з цією особою та попросити її видалити електронний лист (і отримати письмове підтвердження того, що це було зроблено).

Сценарій 3 - Безпечна комунікація

Хоча Лі соромно визнавати, що вона припустилася помилки, вона знає, що найбезпечніше - негайно повідомити про це як про витік даних. Таким чином, особа, яка проводить розслідування, зможе вирішити, чи потрібно зробити більше, і швидко вжити заходів, щоб мінімізувати будь-яку шкоду.

Сценарій 3 - Безпечна комунікація

У рамках цього сценарію ми дізналися про використання безпечних каналів зв'язку, включаючи програми для обміну повідомленнями та зашифровані електронні листи, а також про те, що робити, якщо ви надіслали конфіденційну інформацію неналежному одержувачу.

Ознайомтеся з ключовими моментами, які слід враховувати при виборі каналу зв'язку, вибравши КЛЮЧОВІ МІРКУВАННЯ.

Затверджені інструменти комунікації

KPMG надає користувачам **чати та послуги конференц-зв'язку** для покращення комунікацій та співпраці між співробітниками KPMG.

Для ділового спілкування та співпраці слід використовувати лише схвалені KPMG методи електронного зв'язку (наприклад, **Exchange/Outlook, MS Teams, SharePoint Online**). У розділі "Ресурси" є посилання на глобальний портал "Зовнішня взаємодія" ("External Collaboration"), який містить додаткову інформацію про те, які інструменти схвалені для використання.

Несанкціоновані інструменти (такі як WhatsApp, WeChat, різні соціальні мережі та блоги, DropBox, особистий OneDrive, Google Drive, особиста веб-пошта) ніколи не повинні використовуватися для комунікацій у KPMG, з клієнтами або в рамках проєктів, за винятком випадків, коли це прямо дозволено Національним спеціалістом з питань IT-безпеки (NITSO). Це пояснюється тим, що:

- вони **можуть бути не безпечними** і наражати нас на ризик витоку даних.
- вони можуть порушити **стандарти зберігання даних фірми** або спричиняти передачу інформації через кордони в країни, де місцеве законодавство про конфіденційність даних забороняє таку передачу.

Пам'ятайте про свою відповідальність при користуванні цими послугами

Як і у випадку з усіма формами електронного спілкування, завжди **дбайте про те, щоб зберегти конфіденційність клієнта та поважати особисте життя** в будь-який час. Ви несете загальну відповідальність за те, щоб діяти належним і законним чином.

Використання електронної пошти

Електронна пошта - це бізнес-інструмент, використовуйте його належним чином

Важливо розуміти ризики, пов'язані з використанням електронної пошти в бізнес-цілях, включаючи ризик витоку конфіденційної інформації. Електронна пошта не є захищеною за своєю суттю і не повинна вважатися безпечною - її можуть **пересилати, перехоплювати, роздруковувати та зберігати** інші особи.

Подумайте двічі, перш ніж натиснути "Відправити"

Завжди **ретельно перевіряйте особи одержувачів**, особливо коли надсилаєте електронну пошту зовнішнім користувачам. Рекомендується вимкнути автозаповнення або встановити затримку відправлення.

Щоб зберегти адресу електронної пошти кожного одержувача в таємниці, використовуйте функцію **“Blind CC”** , коли розсилаєте повідомлення великому списку осіб.

Не **обмінюйтеся** конфіденційною інформацією з клієнтом електронною поштою, якщо тільки клієнт не дав чіткого дозволу на використання електронної пошти для листування.

Не **пересилайте** службові повідомлення на особисту електронну пошту та не використовуйте особисту електронну пошту для службових цілей KPMG.

Також не використовуйте адресу електронної пошти KPMG **для неділових цілей**.

Мінімізуйте інформацію **в позаслужбових повідомленнях** – ніколи не розголошуйте інформацію, яка може бути використана ненавмисним одержувачем.

Затверджені інструменти комунікації

Що відбувається, коли я ненавмисно відправляю електронного листа не тій людині?

Негайно повідомте про витік даних згідно з місцевими процедурами, наприклад, повідомивши службу підтримки ITS, щоб можна було вжити необхідних заходів.

Крім того, **зв'яжіться з небажаним одержувачем**, поясніть, що ви надіслали йому щось помилково і попросіть його видалити це і підтвердити електронною поштою, що він це зробив.

Якщо ви надсилаєте конфіденційні інформацію/ дані у вкладених файлах клієнту або іншій третій стороні, **їх потрібно зашифрувати** за допомогою схваленого продукту, наприклад, WinZip.

Паролі повинні відповідати мінімальним вимогам KPMG і мають бути надіслані в окремому повідомленні (через інший носій, наприклад, текстовим повідомленням або телефонним дзвінком).

Конференц-дзвінки та віртуальні наради

Якщо ви проводите віртуальну нараду або телеконференцію, під час якої люди обговорюють важливу або конфіденційну інформацію, необхідно розуміти ризики, пов'язані з цим:

Учасники

Переконайтеся, що на нараді присутні лише **заплановані учасники** , а незапрошені гості не прослуховують розмову.

Голосові записи

Ознайомтеся з політикою вашої фірми-члена, щоб зрозуміти, **що дозволено щодо запису розмов і нарад**, наприклад, повідомляйте про намір записати нараду або обговорення на початку засідання.

Умови і оточення

Усвідомлюйте своє оточення і **уникайте підслуховування,** перемістившись у більш приватну зону.
Якщо ви не можете уникнути підслуховування, повідомте про це іншим учасникам і будьте обережні у висловлюваннях.

Смарт-пристрої

Працюючи з дому, переконайтеся, **що ви не перебуваєте поблизу розумних колонок або голосових помічників**, або переконайтеся, що вони вимкнені.

Коди конференцій

(Якщо це ще застосовується) Пам'ятайте, що код лідера конференц-зв'язку має бути **конфіденційним**, надавайте код учасника лише тим особам, які мають його знати, і періодично змінюйте свої коди.

KPMG

Сценарій 4 – Фішинг, соціальна інженерія та соціальні медіа

Сценарій 4 – Фішинг, соціальна інженерія та соціальні медіа

Ейд і його команда щойно виграли новий великий проєкт.
Він пишається своєю командою і хоче привітати її з досягненнями через соціальні мережі.
Ейд замислюється: його публікацію можуть побачити всі, і він може розповісти занадто багато подробиць про проєкт клієнта. Він не хотів би ділитися надто детальною інформацією про своє особисте життя в соціальних мережах.
Наскільки детально Ейду слід поділитися інформацією про нового клієнта в соціальних мережах?

Сценарій 4 – Фішинг, соціальна інженерія та соціальні медіа

Наскільки детальною інформацією про нового клієнта має поділитися Ейд у соціальних мережах?

A. Він повинен опублікувати повну інформацію про свою роль у KPMG та останній проєкт клієнта, оскільки історії успіху зміцнюють бренд KPMG.

B. Він повинен звести до мінімуму деталі своєї роботи та клієнтських проєктів, наприклад, не згадувати назву клієнта на ім'я або характер роботи, яку він виконує.

Сценарій 4 – Фішинг, соціальна інженерія та соціальні медіа

Наскільки детальною інформацією про нового клієнта має поділитися Ейд у соціальних мережах?

A. Він повинен опублікувати повну інформацію про свою роль у KPMG та останній проєкт клієнта, оскільки історії успіху зміцнюють бренд KPMG.

B. Він повинен звести до мінімуму деталі своєї роботи та клієнтських проєктів, наприклад, не згадувати назву клієнта на ім'я або характер роботи, яку він виконує.

Сценарій 4 – Фішинг, соціальна інженерія та соціальні медіа

Користуючись соціальними мережами, важливо усвідомлювати потенційні ризики та бути обережними з інформацією, якою ви ділитеся, особливо з огляду на те, що контент, який ви публікуєте, ймовірно, побачать не лише ті, кому ви його призначаєте.

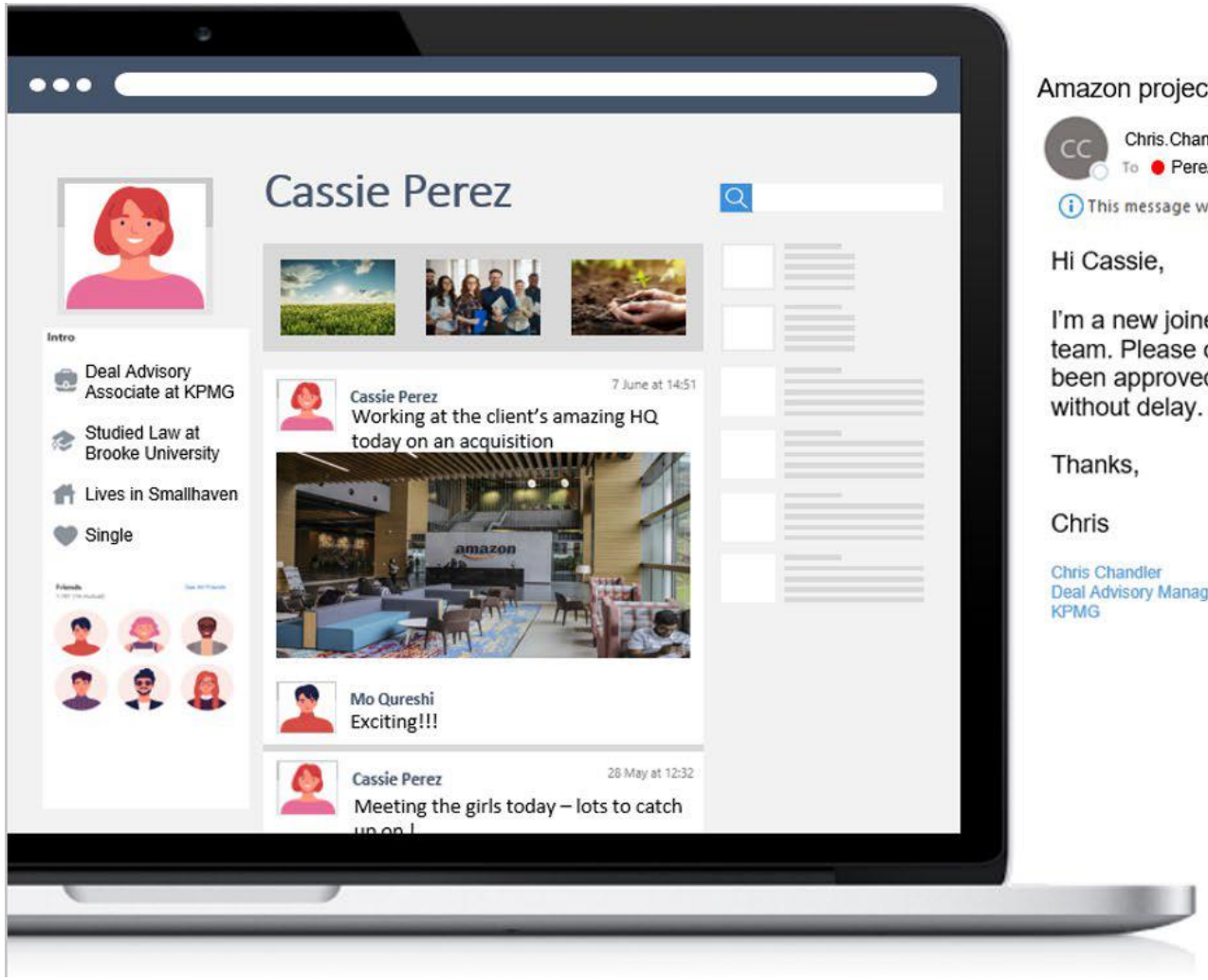
При створенні онлайн-профілю або резюме ніколи не слід надавати занадто багато інформації про свою роль і роботу в KPMG. Це особливо важливо, якщо ви отримуєте доступ до конфіденційної або комерційної інформації, або якщо у вас є привілейований доступ до облікового запису.

Надання занадто великої кількості деталей може порушити конфіденційність, порушити конфіденційність даних інших людей або зробити вас вразливими до атак засобами соціальної інженерії (коли люди стають мішенню для фішингових електронних листів, створених з використанням інформації, поширеної в соціальних мережах, або інших загальнодоступних даних).Завжди переглядайте політику інформаційної безпеки вашої Фірми-члена та інструкції щодо використання соціальних мереж перед публікацією.

Сценарій 4 – Фішинг, соціальна інженерія та соціальні медіа

Ейд передумує ділитися такою кількістю деталей, оскільки це порушило б конфіденційність даних клієнта. Він хоче подати гарний приклад своїй команді щодо безпеки, тому редагує публікацію, щоб видалити деталі про клієнта та характер роботи.

Ви можете визначити ситуації, коли деталями не слід ділитися у соціальних медіа?



Amazon project documentation request

CC Chris.Chandler@kpmg.com
To Perez, Cassie

Reply | Reply All | Forward | ...

Mon 19/06/2023 10:55

This message was sent with High importance.

Hi Cassie,

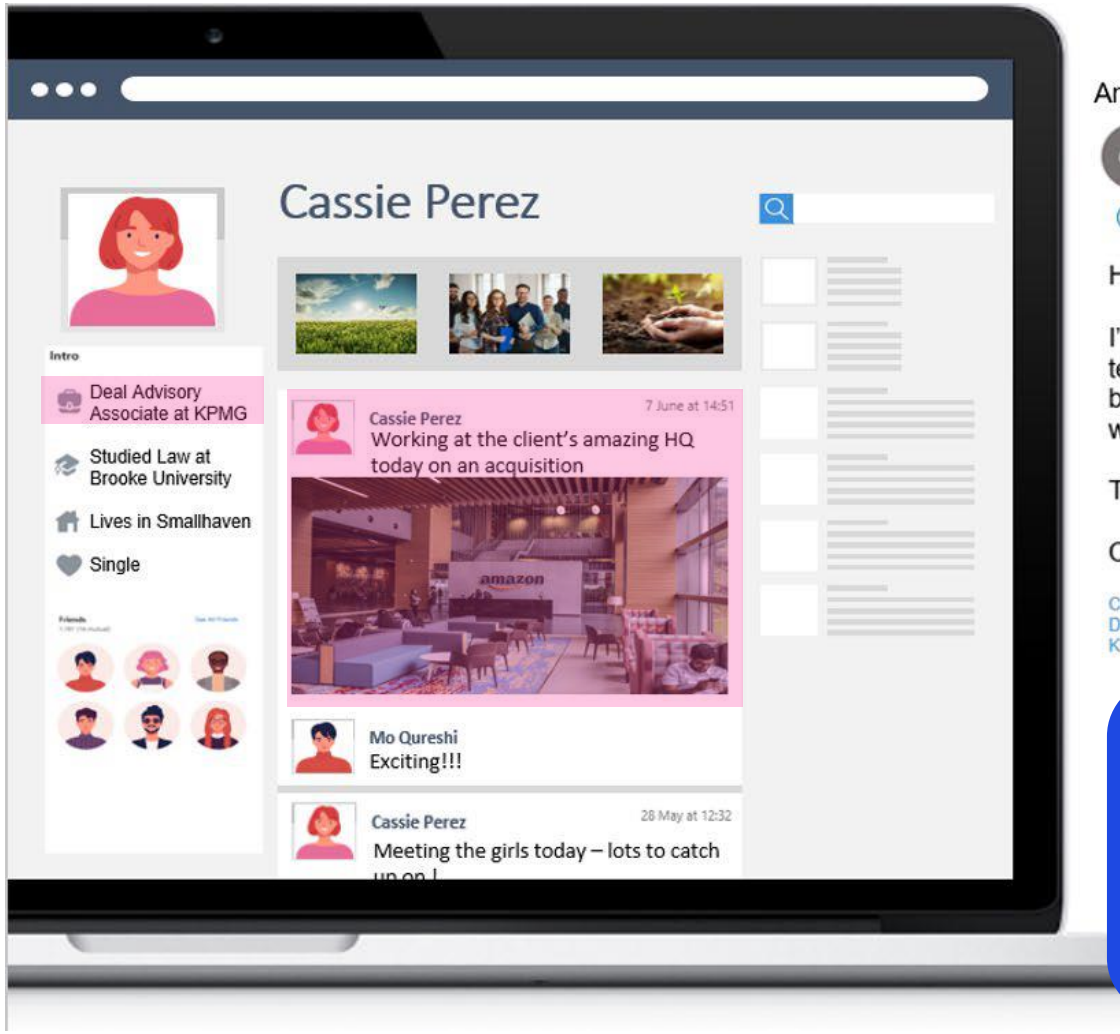
I'm a new joiner in your team and I've just been added to the Amazon Acquisition project team. Please can you urgently send me all available project documentation? This has been approved by senior management, as they need me to begin working on this project without delay.

Thanks,

Chris

Chris Chandler
Deal Advisory Manager
KPMG

Ви можете визначити ситуації, коли деталями не слід ділитися у соціальних медіа?



Amazon project documentation request

Chris.Chandler@kpmg.com
To Perez, Cassie

Reply | Reply All | Forward | ...

Mon 19/06/2023 10:55

This message was sent with High importance.

Hi Cassie,

I'm a new joiner in your team and I've just been added to the Amazon Acquisition project team. Please can you urgently send me all available project documentation? This has been approved by senior management, as they need me to begin working on this project without delay.

Thanks,

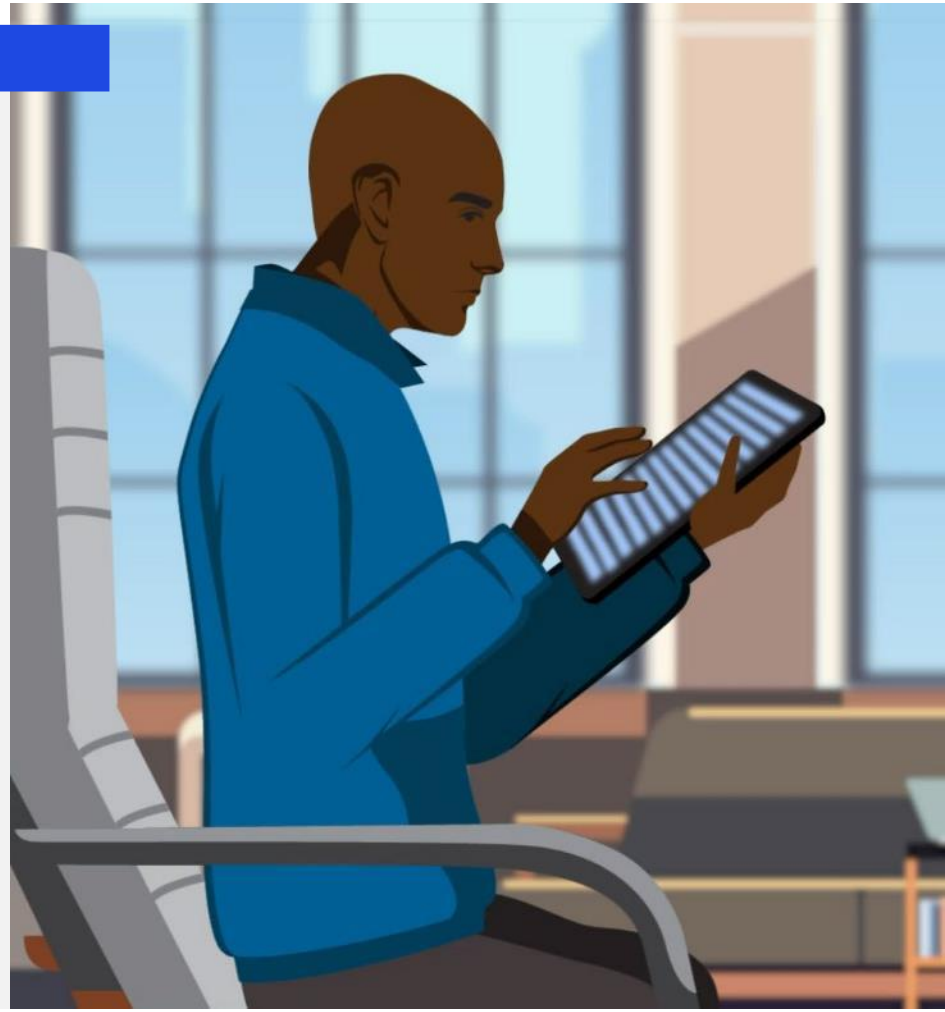
Chris

Chris Chandler
Deal Advisory Manager
KPMG

- Кіберзлочинцю відомо, що Кессі працює у відділі консультування з питань укладання угод у KPMG і наразі працює над угодою з поглинання для Amazon.
- Окремо ці деталі не розкривають багато, але зловмисники можуть зібрати їх разом, щоб створити переконливий цільовий фішинговий лист від імені нового колеги з проханням терміново надіслати йому документацію.
- Зверніть увагу, що домен електронної адреси у фішинговому листі схожий на @kpmg.com, але не зовсім той самий - @kpmq.com.
- Вони також вдаються до наполегливого тону та владного стилю, щоб змусити Кессі надати доступ до файлів.

Сценарій 4 – Фішинг, соціальна інженерія та соціальні медіа

Під час телеконференції в Teams, де він обговорює своє нове завдання, Ейд отримує електронного листа. Схоже, що це запит про витрати від внутрішнього фінансового підрозділу. Лист містить кілька червоних прапорців/підказок, які вказують на те, що він може бути несправжнім.
Ейд зайнятий на зустрічі, але йому цікаво дізнатися більше про проблему з його витратами, тому він обирає вкладення, перш ніж прочитати лист належним чином. Замість документа він бачить смугу завантаження певного повідомлення.
На екрані з'являється повідомлення з вимогою викупу.
Ейд ненавмисно запустив шкідливе програмне забезпечення у вигляді атаки з вимогою викупу, яке тепер може поширитися по всій мережі фірми. У повідомленні вимагається сплатити кошти на криптовалютний гаманець, щоб відновити зашифровані дані та запобігти їх витоку. Що Ейд має робити далі?



Сценарій 4 – Фішинг, соціальна інженерія та соціальні медіа

Що Ейд має робити далі?

A. Негайно відключитися від Wi-Fi, а потім повідомити про атаку як про порушення безпеки.

B. Швидко перезавантажити комп'ютер, а потім видалити електронний лист.

Сценарій 4 – Фішинг, соціальна інженерія та соціальні медіа

Що Ейд має робити далі?

A. Негайно відключитися від Wi-Fi, а потім повідомити про атаку як про порушення безпеки.

B. Швидко перезавантажити комп'ютер, а потім видалити електронний лист.

Сценарій 4 – Фішинг, соціальна інженерія та соціальні медіа

Оскільки це атака з вимогою викупу, яка вже відбувається, він повинен діяти швидко, відключитись від Wi-Fi, а потім повідомити про атаку на окремому пристрої (на випадок таких порушень добре зберігати номер телефону локального каналу зв'язку на мобільному пристрої), або попросити колегу повідомити про це від його імені.

! Не слід вимикати пристрій, оскільки це негативно вплине на судове відновлення нестабільних даних та аналіз шкідливого програмного забезпечення.

Важливо не намагатися впоратися з цим самостійно - дозвольте колегам, які вже мали справу з подібними порушеннями, підказати вам наступні кроки.

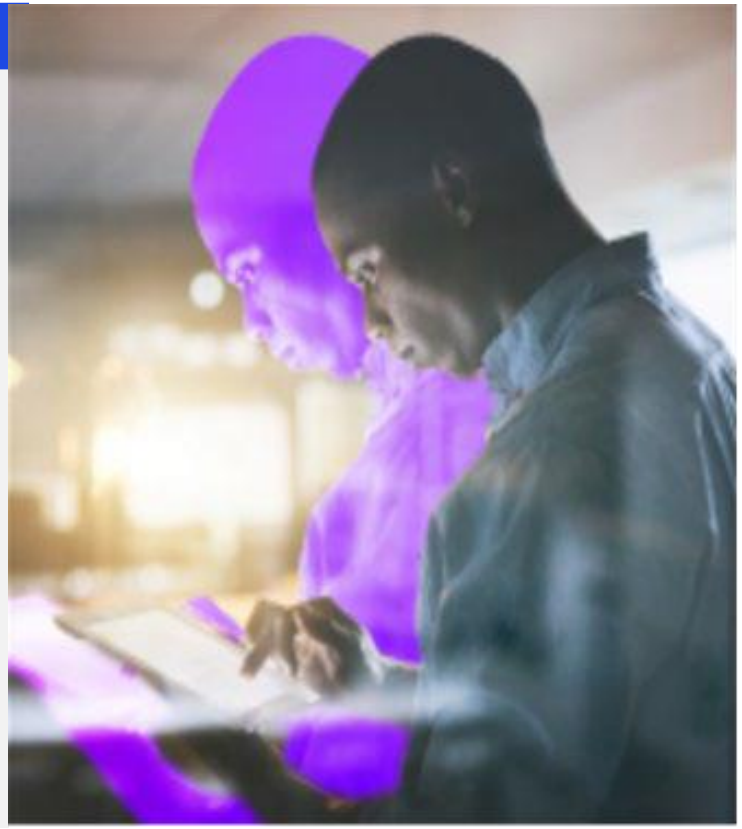
Сценарій 4 – Фішинг, соціальна інженерія та соціальні медіа

Оскільки атака вірусу з вимогами вже відбувається, Ейд має діяти швидко, від'єднавшись від Wi-Fi, а потім повідомити про атаку як про порушення безпеки. Особа, яка проводить розслідування, повідомить Ейда про подальші кроки.

Сценарій 4 – Фішинг, соціальна інженерія та соціальні медіа

У цьому сценарії ви взнали таке:
- приклади надмірного розповсюдження даних в соціальних мережах
- приклади фішингових та онлайн-атак за допомогою засобів соціальної інженерії
- способи протидії атакам з вимогою викупу.

Ознайомтеся з ключовими моментами, які слід враховувати щодо фішингу, соціальної інженерії та безпеки соціальних мереж, вибравши КЛЮЧОВІ МІРКУВАННЯ.



Фішинг

Фішинг - це форма кібератаки, коли зловмисник надсилає шахрайське повідомлення, призначене для того, щоб обманом примусити вас:

- **Розкрити персональну або конфіденційну інформацію,** таку як ваше ім'я користувача KPMG, паролі, персональні ідентифікаційні номери або банківські реквізити
- **Відкрити додаток до листа,** який розгорне шкідливе програмне забезпечення на вашому пристрої
- **Вибрати посилання,** яке скерує вас на фейковий веб-сайт

Фішингові листи: приклад того, на що слід звертати увагу

Фішинг

Як виявити фішингову атаку?

Як співробітники KPMG **ви є цільовою групою** через характер роботи фірми та цінні дані, які ми обробляємо.
Ви можете зменшити ризик стати жертвою, уважно переглядаючи електронну пошту та текстові повідомлення.
Звертайте увагу на такі повідомлення:

- Електронні листи, **які не адресовані особисто вам,** наприклад зі звертанням «Шановний клієнте».
- Електронний лист із запитом **сплатити рахунок-фактуру** чи надати інформацію.
- Електронний лист, який викликає **незвичне/відірване від контексту відчуття терміновості або є** розпливчастим і знеособленим.
- **Орфографічні та граматичні** помилки.
- Електронні листи, **що містять посилання на веб-сторінку або файл** , з якими ви не знайомі. Не натискайте на посилання - замість цього наведіть на нього курсор, щоб побачити URL-адресу. Це надійний спосіб перевірити, чи справжній лист, чи ні.
- Якщо ви отримаєте файл і не знатимете, що це за файл - не відкривайте його. Зокрема, вкладення з розширеннями ".scr", ".com" та ".exe" можуть містити **шкідливе програмне забезпечення або вірус**.
- **Не цілком правильна адреса електронної пошти** - вона може використовувати ім'я когось із ваших знайомих або знайомої компанії, але буде дещо відрізнятися. Перевіряйте адресу електронної пошти, щоб переконатися, що вона автентична.
- Електронний лист із вимогою **активувати або тимчасово призупинити фінансовий рахунок**, змінити пароль або спосіб оплати, а також з проханням ввести персональні або банківські реквізити. Перш ніж надавати будь-яку персональну або ділову інформацію, перевіряйте джерело та сайт.

Якщо ви отримаєте підозрілий фішинговий лист на свою поштову скриньку, **не переходьте за жодними посиланнями та не відкривайте жодних вкладень, що містяться в листі**. І не пересилайте такого листа колегам.

Якщо ваша Фірма-член **має кнопку повідомлення про фішинг** в Outlook, скористайтеся нею, щоб повідомити про фішинг. В іншому випадку дотримуйтесь процесу звітування у вашій Фірмі-члені, наприклад, зверніться до служби підтримки ITS.

Соціальна інженерія

Що таке "Соціальна інженерія"?

Соціальна інженерія — це технологія, яка використовується для **зловживання довірчими стосунками** і кращими якостями людської природи, таких як наша схильність бути корисними, **щоб обманом змусити вас розкрити цінну інформацію** про себе чи фірму.

Ніколи не надавайте особисту інформацію або конфіденційну інформацію про себе, своїх колег, фірму або наших клієнтів, якщо ви не впевнені, що ваш співрозмовник має право на її отримання.

Переконайтеся, що ця особа має право запитувати цю інформацію, і що вона є саме тим, за кого себе видає.

Остерігайтеся таких атак

- Коли вони починають свою атаку, вони видають себе за **надійне джерело** та можуть звертатися до вас на ім'я, щоб додати вигляду автентичності.
- Вони можуть звернутися до вас через **соціальні мережі,** такі як LinkedIn, пропонуючи можливість ділового або публічного виступу і використовуючи такий спосіб збору конфіденційної інформації.
- Їхній контакт може здійснюватися через **особисту взаємодію**, наприклад, телефонний дзвінок або особисту зустріч.
- Вони можуть попросити **назвати імена колег з** KPMG, або надати їм довідник KPMG.
- **"Списовий фішинг" (“Spear phishing”)** - це електронні листи, націлені на конкретних людей, в яких використовується інформація про потенційних жертв, зібрана з соціальних мереж або інших загальнодоступних даних, наприклад, інформація про конференції, які ви відвідуєте, ваші професійні інтереси тощо).

Відео- та аудіо-діпфейки – штучні носії інформації, що замінюють людину на її подобу або "клонований" голос - можуть бути використані в шахрайстві з використанням соціальної інженерії, коли люди думають, що отримали інструкції від людини, якій вони довіряють, з проханням переказати гроші на банківський рахунок.

Уникайте шахрайських **телефонних дзвінків, електронних листів, SMS або повідомлень у соціальних мережах** від зловмисників, які видають себе за ваших знайомих. Завжди перевіряйте окремо з таку особу, перш ніж перераховувати гроші.

Соціальні мережі

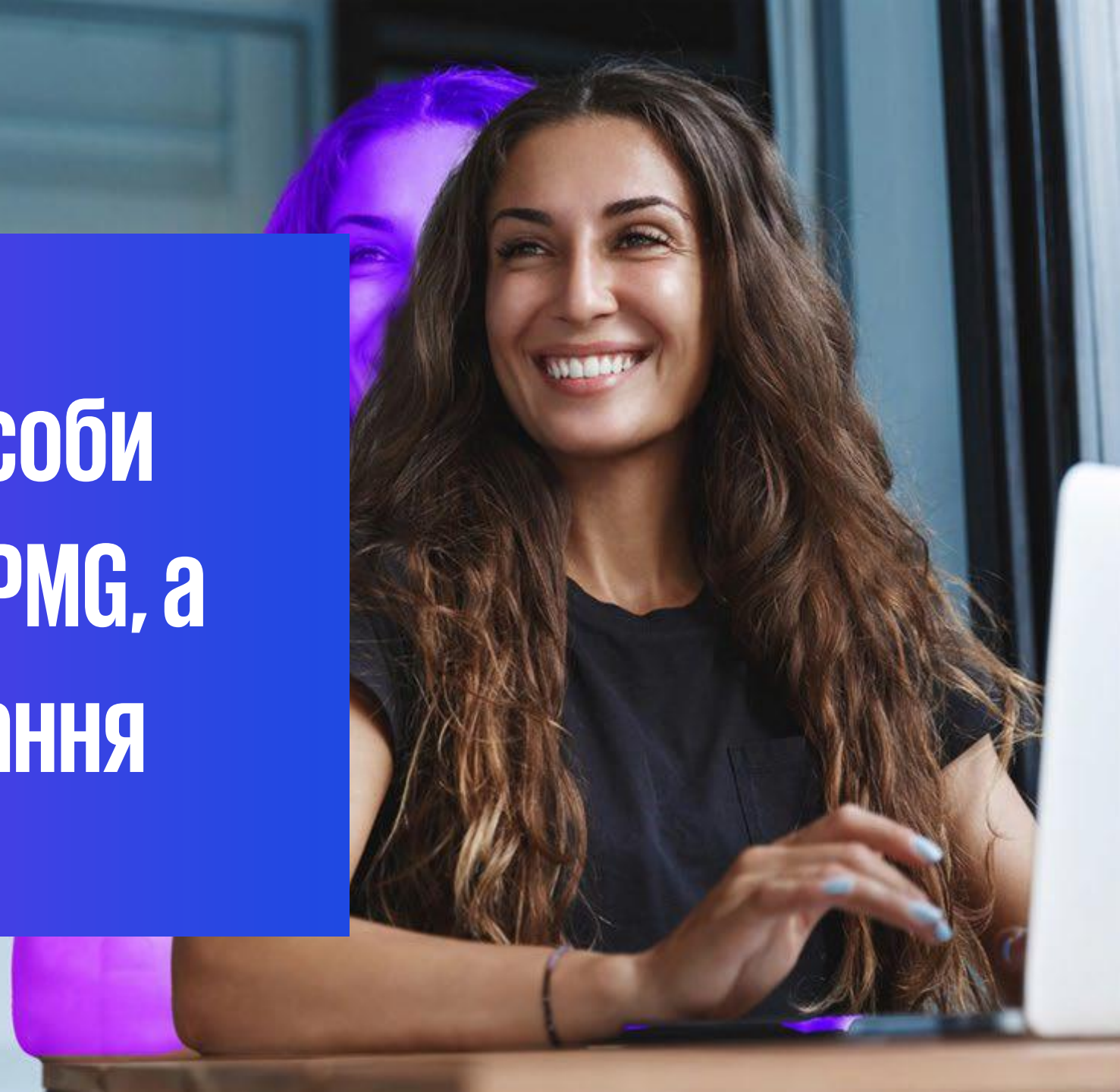
Користуючись соціальними мережами, важливо усвідомлювати **потенційні ризики** та бути обережними з інформацією, якою ви ділитеся, особливо з огляду на те, що контент, який ви публікуєте, ймовірно, побачать не лише ті, кому ви його призначаєте.

Ми всі несемо особисту та професійну відповідальність **за захист конфіденційності клієнтів**, **повагу** до інших людей та їхнього приватного життя, а також найвищу повагу до **репутації та цінностей KPMG** під час використання внутрішніх та зовнішніх соціальних мереж.

Перегляданте політику інформаційної безпеки вашої Фірми-члена та інструкції щодо використання соціальних мереж перед публікацією. Крім того, дотримуйтесь наступних кращих практик:

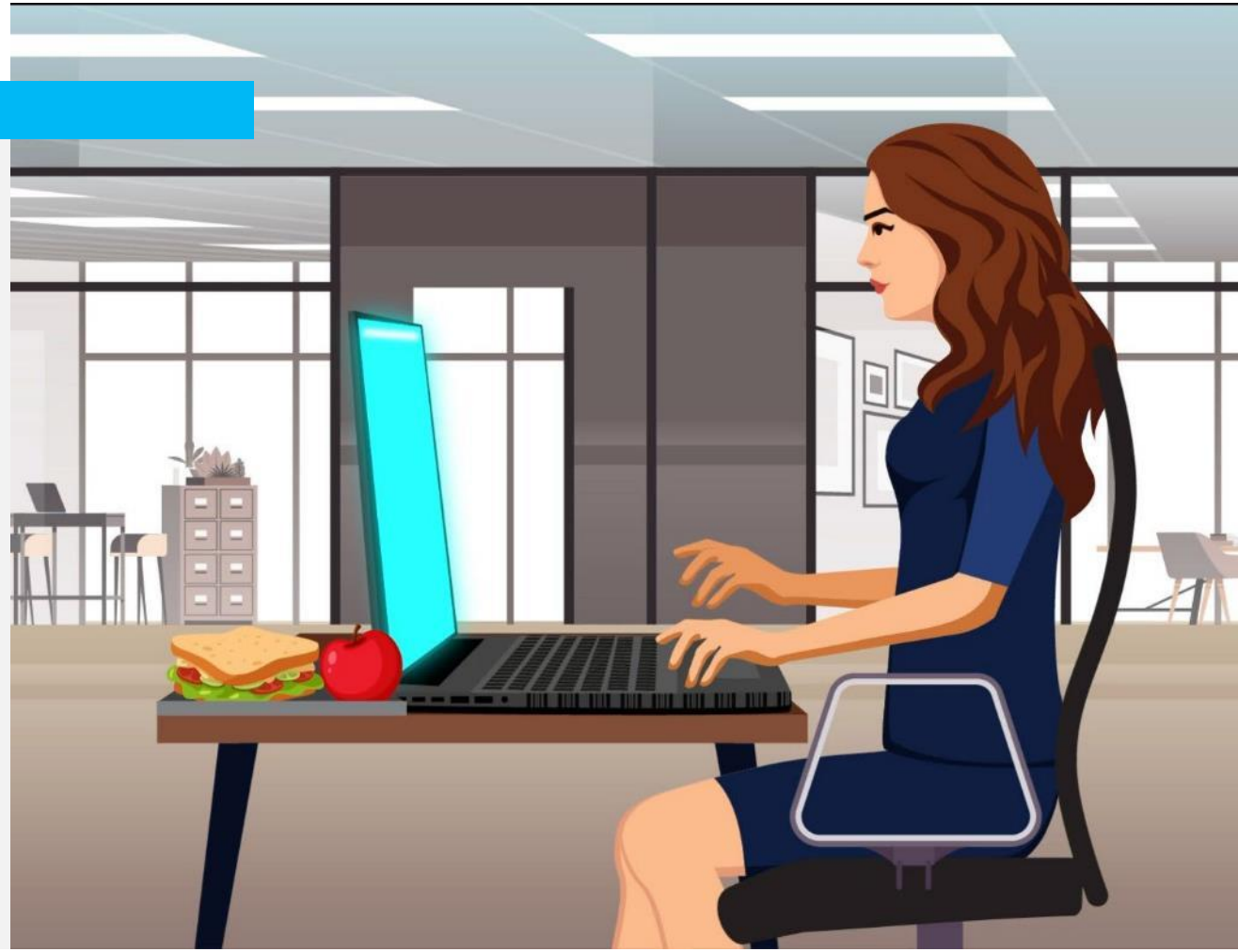
- Ознайомтеся з політикою конфіденційності та **налаштуваннями безпеки** кожного сайту та вносьте необхідні корективи.
- Не публікуйте та не посилайтеся на матеріали, **які є наклепницькими, образливими або непристойними**.
- Не використовуйте той самий **пароль** який ви використовуєте в мережі KPMG або на інших сайтах, оскільки якщо один сайт буде зламаний, ваш розкритий пароль може бути використаний для доступу до ваших облікових записів на інших сайтах. І не використовуйте свою **електронну адресу KPMG** у соціальних мережах, якщо це не потрібно для професійних цілей.
- Створюючи онлайн-профіль або резюме, не повідомляйте занадто багато деталей **про свою роль у KPMG та професійну діяльність** - це особливо важливо, якщо ви маєте доступ до суворо конфіденційної або службової інформації, а також якщо у вас є привілейований обліковий запис.
- Не діліться інформацією, яка може завдати шкоди **репутації KPMG**, а також не пропонуйте поради та не надавайте інформацію, які можуть бути витлумачені як офіційна ділова консультація від KPMG.

Сценарій 5 – Інформаційні засоби та обладнання KPMG, а також використання інструментів ШІ



Сценарій 5 – Інформаційні засоби та обладнання KPMG, а також використання інструментів ШІ

Софія була зайнята весь ранок, але зараз настав час обіду, і вона йде на заслужену перерву. Під час обідньої перерви вона любить переглядати новини та користуватися інтернетом.



На які з цих веб-сайтів доречно заходити на пристрої KPMG?

Веб-сайти азартних ігор

Facebook

Google

Wikipedia

Порнографічні сайти

Веб-сайти, що містять інформацію про незаконну діяльність або заохочують її

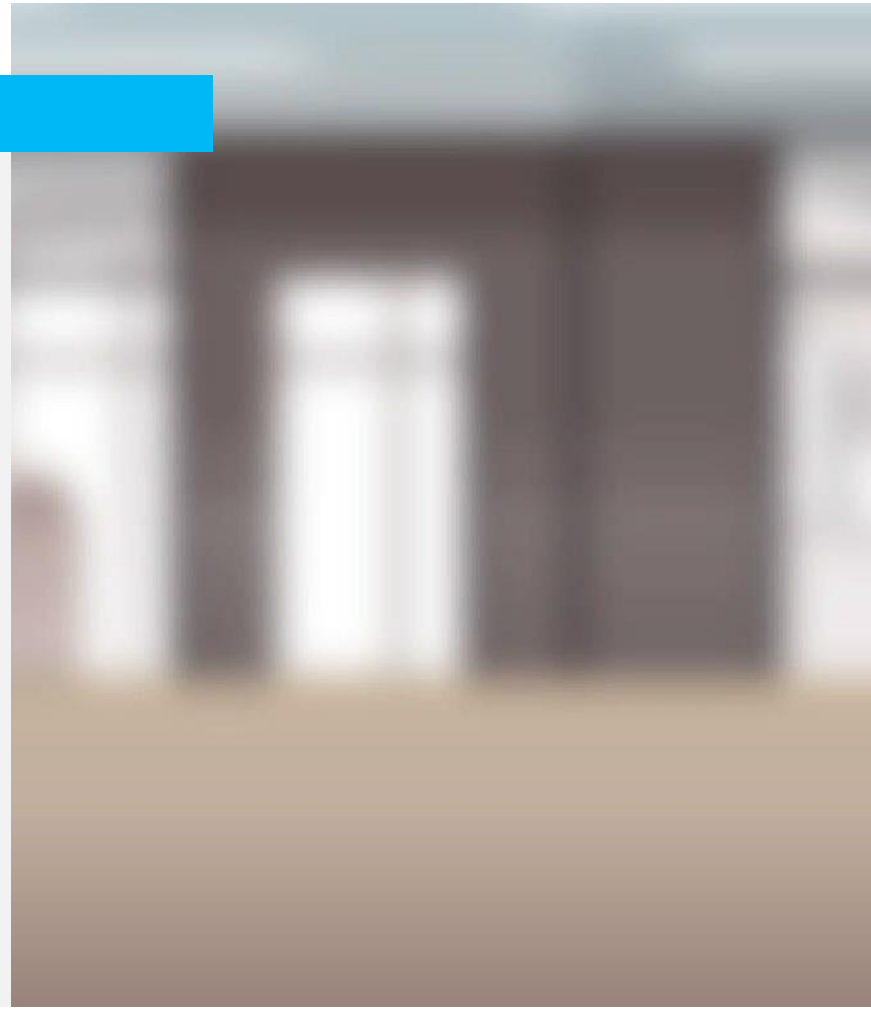
Відповідь:

ТАК	НІ
Facebook	Веб-сайти азартних ігор
Google	Порнографічні сайти
Wikipedia	Веб-сайти, що містять інформацію про незаконну діяльність або заохочують її

Сценарій 5 – Інформаційні засоби та обладнання KPMG, а також використання інструментів ШІ

Софія також любить контролювати свій онлайн-бізнес. У вільний час вона виготовляє ювелірні прикраси і продає їх через онлайн-платформу. Вона щойно почала користуватися новим додатком, який просуває її оголошення в соціальних мережах і має допомогти збільшити продажі. Софія використовує цю програму на своєму домашньому ноутбуці, але вона думає, що було б зручно завантажити її і на свій робочий ноутбук. Вона вагається, оскільки не впевнена, чи можна завантажувати додаток для особистого користування на ноутбук KPMG. Чи повинна Софія завантажити додаток?

.



Сценарій 5 – Інформаційні засоби та обладнання KPMG, а також використання інструментів ШІ

Чи слід Софії завантажувати програму?

A. Ні, оскільки вона не отримала дозволу на завантаження програми.

B. Так, оскільки вона планує користуватися нею лише під час обідньої перерви, тож це не буде заважати її роботі. Дозволяється обмежене використання пристроїв KPMG в особистих цілях.

Сценарій 5 – Інформаційні засоби та обладнання KPMG, а також використання інструментів ШІ

Чи слід Софії завантажувати програму?

A. Ні, оскільки вона не отримала дозволу на завантаження програми.

B. Так, оскільки вона планує користуватися нею лише під час обідньої перерви, тож це не буде заважати її роботі. Дозволяється обмежене використання пристроїв KPMG в особистих цілях.

Сценарій 5 – Інформаційні засоби та обладнання KPMG, а також використання інструментів ШІ

Якщо ви захочете встановити нове програмне забезпечення на пристрій KPMG, вам необхідно буде отримати дозвіл від вашого місцевого відділу ITS (який може провести консультацію з Національним спеціалістом з питань IT-безпеки (NITSO) або місцевим Підрозділом управління ризиками) та надати обґрунтовану бізнес-аргументацію. Несанкціоноване програмне забезпечення може становити загрозу для мережі та систем KPMG (наприклад, якщо воно містить шкідливий код, який може спричинити витік інформації або втрату даних).

І хоча прийнятне використання в особистих цілях може бути дозволено (відповідно до місцевих правил Фірми-члена), ви не повинні використовувати системи або пристрої KPMG для власної вигоди (наприклад, для ведення власного бізнесу) або встановлювати програмне забезпечення для особистого використання на пристроях KPMG (за винятком випадків, коли це спеціально дозволено вашою Фірмою-членом).

Слід також зазначити, що співробітники KPMG повинні зв'язатися з відділом з питань етики та незалежності щодо отримання дозволу на ведення власного бізнесу в неробочі години KPMG.

Сценарій 5 – Інформаційні засоби та обладнання KPMG, а також використання інструментів ШІ

Софія вважає, що краще розмежувати її власний бізнес та роботу. Натомість вона може завантажити додаток на свій мобільний телефон, якщо їй потрібно попрацювати над ним під час обіду. Пізніше вона починає збиратися додому. Вона планує попрацювати на вихідних, але не хоче нести свій ноутбук додому. Вона вирішує зберегти документи, над якими працювала, на зашифровану флешку. Тепер Софія може закінчити роботу вдома, на своєму особистому пристрої. Але вона не впевнена, чи варто це робити - файли, які вона забирає додому, містять конфіденційні кадрові дані про співробітників KPMG. Можливо, їй слід спочатку отримати дозвіл? Чи потрібно Софії отримати дозвіл на використання зашифрованої флешки для передачі конфіденційної інформації?

Сценарій 5 – Інформаційні засоби та обладнання KPMG, а також використання інструментів ШІ

Чи потрібно Софії отримувати дозвіл на використання зашифрованого USB-накопичувача для передачі конфіденційної інформації?

A. Ні, це не обов'язково, оскільки це не надто великий ризик. Пристрій зашифрований і буде містити лише конфіденційну інформацію KPMG, а не конфіденційну інформацію клієнта або інформацію KPMG з високим ступенем конфіденційності.

B. Так, вона повинна отримати дозвіл, якщо хоче використовувати USB-накопичувач для перенесення конфіденційної інформації KPMG на свій персональний пристрій для роботи.

Сценарій 5 – Інформаційні засоби та обладнання KPMG, а також використання інструментів ШІ

Чи потрібно Софії отримувати дозвіл на використання зашифрованого USB-накопичувача для передачі конфіденційної інформації?

A. Ні, це не обов'язково, оскільки це не надто великий ризик. Пристрій зашифрований і буде містити лише конфіденційну інформацію KPMG, а не конфіденційну інформацію клієнта або інформацію KPMG з високим ступенем конфіденційності.

B. Так, вона повинна отримати дозвіл, якщо хоче використовувати USB-накопичувач для перенесення конфіденційної інформації KPMG на свій персональний пристрій для роботи.

Сценарій 5 – Інформаційні засоби та обладнання KPMG, а також використання інструментів ШІ

Ви ніколи не повинні переносити або зберігати конфіденційну інформацію KPMG або Клієнта на будь-якому власному або сторонньому устаткуванні чи сервісі без дозволу IT-служби Вашої Фірми-члена (ITS), Національного спеціаліста з питань IT-безпеки (NITSO) та локального підрозділу управління ризиками.

Використання USB-накопичувачів категорично не рекомендується, але за відсутності альтернативи слід використовувати тільки схвалений KPMG пристрій, зашифрований за допомогою схваленого рішення. Також слід бути обережним при транспортуванні конфіденційної інформації, оскільки невеликі портативні пристрої зберігання даних можна легко загубити, вони можуть бути вкрадені або розміщеними в неналежному місці. Про таке порушення можуть повідомити ЗМІ, що може призвести до значних штрафів або навіть професійного осуду, що завдасть шкоди бренду та репутації KPMG.

Сценарій 5 – Інформаційні засоби та обладнання KPMG, а також використання інструментів ШІ

Софія обговорює це зі своїм менеджером. Її менеджер просить її не забирати файли додому, а закінчити роботу наступного тижня в офісі і насолоджуватися вихідними.

Сценарій 5 – Інформаційні засоби та обладнання KPMG, а також використання інструментів ШІ

У цьому сценарії ви дізналися про таке:
- на які веб-сайти доречно заходити на пристрої KPMG,
- правила встановлення програмного забезпечення та використання пристроїв KPMG в особистих цілях,
- належне використання знімних носіїв інформації.

Виберіть КЛЮЧОВІ МІРКУВАННЯ, щоб дізнатися більше про безпечне використання інформаційних засобів та обладнання KPMG і прийнятне використання інструментів ШІ.

Використання Інтернету

Користуючись Інтернетом або електронними засобами зв'язку за допомогою IT-ресурсів KPMG, дуже важливо **діяти розсудливо,** щоб не поставити під загрозу репутацію KPMG.

Ви ніколи не повинні **отримувати доступ, поширювати, створювати або публікувати неприйнятний контент** при використанні пристроїв KPMG. Якщо вас спіймають на таких діях, як ви, так і ваша Фірма-член можуть стати об'єктами судових позовів, штрафів, репутаційних збитків або інших заходів.

Неприйнятний контент включає будь-які форми письмових матеріалів, фотографії, зображення або відеоконтент, а також посилання на інтернет-сайти, які можуть вважатися образливими, незаконними, загрозливими або з інших причин неприйнятними в професійному середовищі (наприклад, расові або сексуальні домагання, наклепницькі матеріали, небажані комерційні або політичні повідомлення).

You should also never access and/or interact with inappropriate websites (unless required for business reasons):

Веб-сайти азартних ігор

Веб-сайти, що містять інформацію про незаконну діяльність або заохочують її

Порнографічні сайти

Інші веб-сайти, які можуть зашкодити репутації KPMG

Інші категорії веб-сайтів, які можуть становити ризик через відому загрозу, інформація про яку надана Національним спеціалістом з питань IT-безпеки (NITSO) або місцевим підрозділом ITS

Використання затвердженого програмного забезпечення

Затверджене програмне забезпечення - це програмне забезпечення, **яке було перевірено та схвалено** для використання в робочих цілях на пристроях KPMG.

Пристрої KPMG комплектуються стандартним набором затвердженого програмного забезпечення, яке пройшло відповідну оцінку ризиків, щоб гарантувати, що воно не становить загрози для мережі та систем KPMG (наприклад, щоб гарантувати, що воно не містить шкідливого коду, який може спричинити витік інформації/даних або втрату даних).

Якщо ви захочете **встановити нове програмне забезпечення** на пристрій KPMG, вам необхідно буде отримати дозвіл від вашого місцевого відділу ITS (який може провести консультацію з Національним спеціалістом з питань IT-безпеки (NITSO) або місцевим Підрозділом управління ризиками) та надати обґрунтовану бізнес-аргументацію.

Не припускайте, що оскільки певне програмне забезпечення було схвалене для одного **проєкту/завдання**, то його можна використовувати для вашого проєкту - ризики можуть бути зовсім іншими, наприклад, в частині конфіденційності даних, які будуть зберігатися в певному інструменті.

Якщо ви вже встановили програмне забезпечення, яке ще не було оцінене та схвалене, **негайно видаліть його** до отримання схвалення (або ж Національний спеціаліст з питань IT-безпеки може запропонувати схвалену альтернативу, яку ви зможете використати натомість).

Якщо ви встановили нове програмне забезпечення для роботи з клієнтом, **обов'язково видаліть його, як тільки воно стане непотрібним**, щоб відновити стандартну конфігурацію KPMG на вашому пристрої

Використання затвердженого програмного забезпечення

Несанкціоновані послуги третіх осіб

Сторонні сервіси, такі як DropBox, особистий OneDrive, Google Drive, особиста веб-пошта, WhatsApp, Siri та Google Translate, **не повинні використовуватися** для обробки інформації KPMG або клієнтів без прямого дозволу місцевого Національного спеціаліста з питань IT-безпеки.

Генеративний ШІ

Використання будь-якої послуги або інструменту штучного інтелекту вважається послугою третьої сторони **і як таке заборонено глобальною політикою, якщо тільки це не схвалено у прямій формі** Національним спеціалістом з питань IT-безпеки фірми-члена.

Фірми-члени, які розглядають можливість використання послуг та/або інструментів генеративного ШІ (включаючи, наприклад, ChatGPT, Bard і Dall_E2), повинні спочатку проконсультуватися зі своїм Національним спеціалістом з питань IT-безпеки (спільно з місцевим підрозділом з управління ризиками), а також дотримуватися **процедури оцінки ризиків** фірми-члена, відповідно до запропонованого варіанту використання.

Безпечне використання IT-ресурсів та обладнання KPMG

Особисте обладнання

Якщо ваша місцева фірма-член KPMG підтримує програму **Bring Your Own Device (BYOD)**для ноутбуків або мобільних пристроїв (планшетів або смартфонів), переконайтеся, що ви дотримуєтеся всіх місцевих правил і практик, пов'язаних з реєстрацією та використанням вашого пристрою для цілей KPMG. Здійснюйте резервне копіювання даних KPMG з ноутбука або мобільного пристрою лише на надане або затверджене KPMG сховище.

Обладнання від сторонніх виробників

Не переносьте і не зберігайте конфіденційну інформацію KPMG на **будь-якому власному або сторонньому устаткуванні чи сервісі** без належного дозволу, наприклад IT-служби (ITS), Національного спеціаліста з IT-безпеки (NITSO) та/або місцевого підрозділу управління ризиками. У випадку отримання дозволу вживайте необхідних заходів для забезпечення належного захисту інформації від втрати або несанкціонованого доступу.

Використання в ділових цілях та в особистих цілях

Фірми-члени KPMG можуть дозволяти використання IT та інформаційних активів KPMG в особистих цілях (відповідно до місцевих правил фірми-члена), якщо це є **обґрунтованим** і не порушує міжнародну або місцеву політику KPMG:

- Переконайтеся, що ви не споживаєте **надмірних ресурсів** (наприклад, при тривалому зберіганні особистих файлів на пристроях/серверах KPMG)
- Не використовуйте системи KPMG для отримання **особистої вигоди** (наприклад, для ведення власного бізнесу)
- Переконайтеся, що особисте використання не впливає на індивідуальну **продуктивність** та не перешкоджає будь-якій діловій діяльності KPMG
- Не встановлюйте **програмне забезпечення для особистого використання** на пристроях KPMG (за винятком випадків, коли це спеціально дозволено вашою фірмою-членом)

Безпечне використання IT-ресурсів та обладнання KPMG

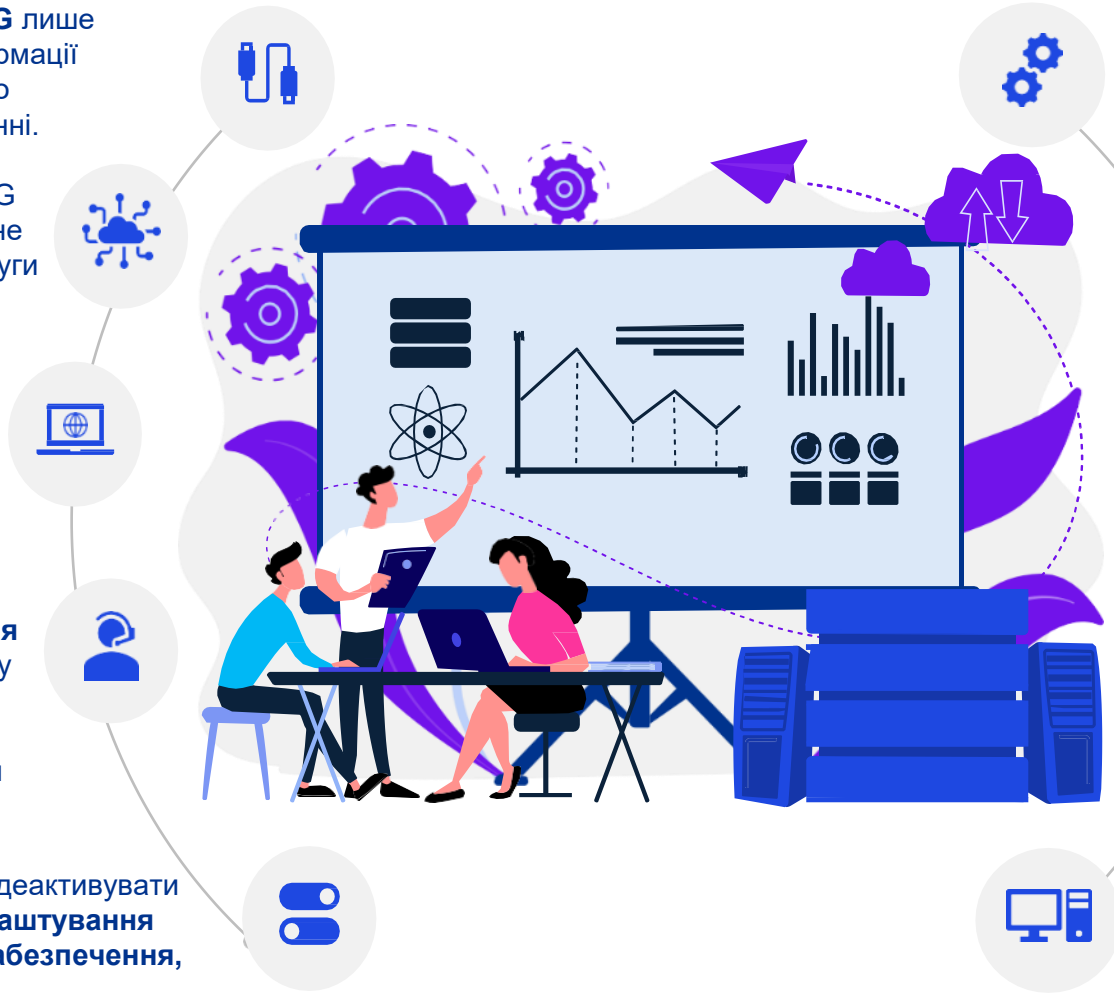
Використовуйте **пристрої KPMG** лише для зберігання та обробки інформації KPMG та інформації клієнтів, що знаходиться на нашому зберіганні.

Не підключайте до мережі KPMG **несанкціоновані пристрої** та не активуйте несанкціоновані послуги (наприклад, бездротові точки доступу).

Регулярно підключайте свій ноутбук до мережі KPMG, щоб встановлювати **оновлення безпеки та програмного забезпечення.**

Якщо **програмне забезпечення або функції безпеки** на вашому ноутбуці не оновлені або не працюють належним чином, звертайтеся до місцевої служби підтримки (ITS).

Не намагайтеся змінювати або деактивувати **будь-яку конфігурацію та налаштування апаратного чи програмного забезпечення,** наданого KPMG.



Для ремонту та обслуговування пристроїв KPMG звертайтеся лише до служби підтримки ITS – ніколи не звертайтеся **до сторонньої майстерні з ремонту IT-обладнання.**

Не пересилайте пристрої KPMG без належного захисту (наприклад, використовуйте **затверджену кур'єрську службу**).

Якщо ваша фірма-член дозволяє використовувати **зашифровані пристрої зберігання даних**, використовуйте тільки захищені паролем пристрої, схвалені KPMG.

Якщо ви плануєте **записати онлайн-зустріч**, переконайтеся, що ви використовуєте лише схвалені програми та пристрої для запису.

Завжди зберігайте пристрої та знімні носії інформації KPMG **у безпеці, перебуваючи в офісі або у віддаленому місці**.

Мобільні пристрої та додатки

Дотримуйтесь таких рекомендацій щодо безпечного використання мобільних пристроїв, щоб запобігти ризику витоку або втрати інформації та даних KPMG, клієнта, а також вашої особистої інформації та даних:

Для доступу до інформації та систем KPMG використовуйте **тільки** схвалені KPMG мобільні пристрої.

Не редагуйте та не зберігайте конфіденційні документи KPMG або клієнтів на персональному пристрої.

Зважте, чи потрібно вам зберігати будь-які персональні дані на пристрої KPMG: фірма KPMG залишає за собою право "віддаленого стирання" будь-якого мобільного пристрою, що використовується для цілей KPMG, що може спричинити втрату таких даних.

Ніколи не використовуйте "зламані", "рутовані" або аналогічно скомпрометовані пристрої для цілей KPMG.

Не змінюйте та не відключайте жодних конфігурацій та налаштувань на вашому мобільному пристрої KPMG.

Обирайте складний для вгадування пароль пристрою - уникайте використання цифр і букв, що повторюються, або послідовностей, які легко вгадати.

Регулярно оновлюйте програмне забезпечення: встановлення останньої версії операційної системи та додатків допоможе захистити ваш пристрій від більшості відомих загроз.

Віддавайте свій пристрій KPMG для ремонту **тільки** представникам місцевої служби ITS, ніколи не передавайте його сторонньому магазину наприклад, магазину Apple.

Захищайте свій пристрій під час подорожей - тримайте його з собою, коли це можливо, а в інший час зберігайте його в надійному місці.

Завантажуйте додатки лише з перевірених джерел, таких як офіційні магазини додатків Apple або Google

Завжди тримайте його в безпеці

Завжди блокуйте екран, коли залишаєте мобільний пристрій без нагляду на короткий час вдома чи в офісі KPMG.

Замикайте його, якщо він не використовується протягом тривалого періоду часу.

Негайно повідомляйте про втрачений або викрадений пристрій відповідно до місцевих процедур або політик.

Сценарій 6 – Працюйте безпечно, де б ви не знаходилися

Сценарій 6 – Працюйте безпечно, де б ви не знаходилися

Зайнаб працює зранку вдома, а пізніше йде до офісу. Чи можете ви визначити безпекові ризики, пов'язані з роботою вдома?

Сценарій 6 – Працюйте безпечно, де б ви не знаходилися

1. Вона відповідає на конфіденційний робочий дзвінок по мобільному телефону, який можуть чути інші люди в кімнаті
2. Поруч з нею знаходиться активний розумний пристрій
3. В неї за спиною стоїть чоловік, дивлячись на деталі на екрані її ноутбука
4. Пароль від Wi-Fi маршрутизатора написаний на стікері
5. На робочому столі залишився документ з грифом "конфіденційно"
6. У кошику для сміття лежить документ з грифом "конфіденційно"
7. На столику біля дверей залишено носій даних

Сценарій 6 – Працюйте безпечно, де б ви не знаходилися

По дорозі до офісу Зайнаб вирішує перекусити в найближчій кав'ярні. Чи можете ви визначити безпекові ризики, пов'язані з перебуванням в такому місці?

Сценарій 6 – Працюйте безпечно, де б ви не знаходилися

1. Вона відповідає на конфіденційний робочий дзвінок по мобільному телефону, який можуть чути інші люди в кімнаті
2. Поруч з нею знаходиться активний розумний пристрій
3. В неї за спиною стоїть чоловік, дивлячись на деталі на екрані її ноутбука
4. Пароль від Wi-Fi маршрутизатора написаний на стікері
5. На робочому столі залишився документ з грифом "конфіденційно"
6. У кошику для сміття лежить документ з грифом "конфіденційно"
7. На столику біля дверей залишено носій даних

Сценарій 6 – Працюйте безпечно, де б ви не знаходилися

Зайнаб приходить до офісу KPMG на післяобідній семінар. Чи можете ви визначити безпекові ризики в офісі KPMG?

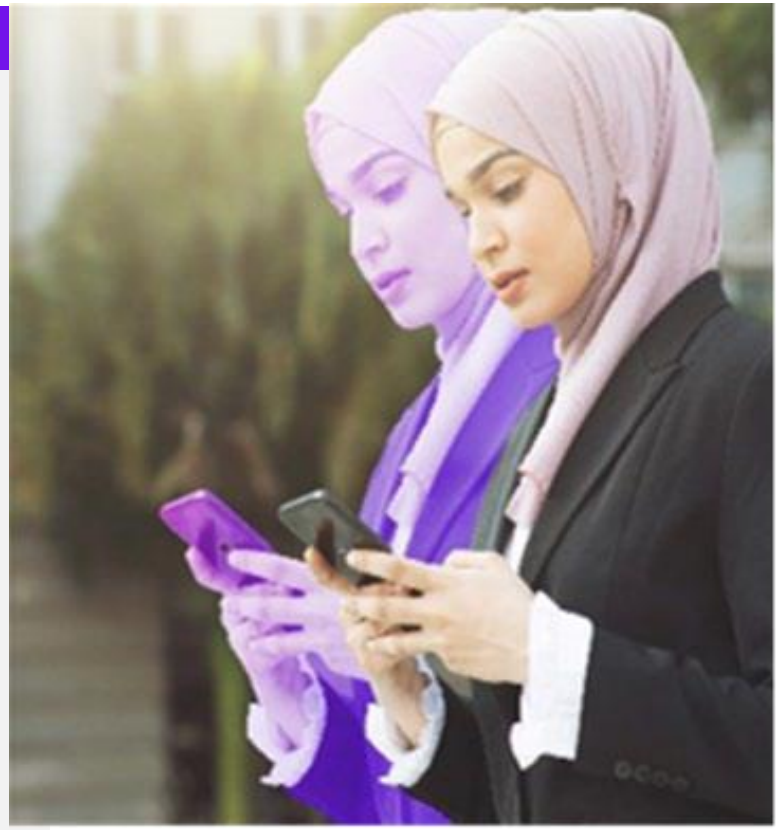
Сценарій 6 – Працюйте безпечно, де б ви не знаходилися

1. Людина без бейджа намагається увійти до офісу позаду Зейнаб
2. На столі залишено без нагляду ноутбук із незаблокованим екраном
3. Ідентифікатор для входу та пароль можна побачити на стікері, прикріпленому до столу
4. В незачиненій шафі залишено конфіденційні документи
5. Мобільний пристрій залишено без нагляду на столі
6. Двоє людей ведуть конфіденційну розмову, яку можуть чути колеги
7. На дошці залишилася конфіденційна інформація про проєкт клієнта
8. Документи з грифом "конфіденційно" залишені без нагляду на принтері
9. Конфіденційний документ був викинутий у загальний кошик для сміття замість захищеного контейнера для утилізації, що стоїть поруч

Сценарій 6 – Працюйте безпечно, де б ви не знаходилися

У цьому сценарії ви дізналися про ризики інформаційної безпеки при роботі вдома, в офісі та в дорозі.

Ознайомтеся з ключовими моментами, які слід враховувати для цілей безпечної роботи, вибравши КЛЮЧОВІ МІРКУВАННЯ.



Працюйте безпечно вдома

Ми всі відіграємо важливу роль у гарантуванні **безпеки інформації та пристроїв** під час роботи вдома:

Повністю вимикайте свій ноутбук KPMG в кінці кожного робочого дня (це ускладнює крадіям доступ до нього) і надійно замикайте його. Не дозволяйте нікому з ваших рідних користуватися ним.

Регулярно підключайтеся до мережі KPMG, щоб отримувати автоматичні оновлення безпеки, що містять виправлення, які захищають ваш пристрій.

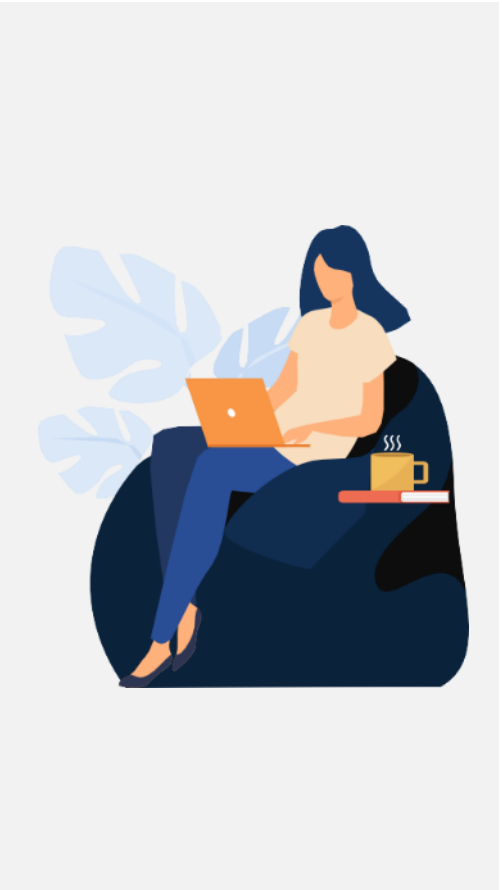
Слідкуйте за тим, щоб ніхто з членів вашої родини не міг переглядати документи KPMG та клієнтів - тримайте їх подалі від сторонніх очей і прибирайте, коли закінчуєте роботу над ними.

Не викидайте конфіденційні документи KPMG або клієнтів разом зі звичайним побутовим сміттям, якщо вони не були попередньо подрібнені. Ви можете використовувати власний **перехресний шредер**, якщо він відповідає стандарту безпеки DIN 66399, рівень 4 або вище.

Якщо обговорюється дуже конфіденційна або чутлива інформація, подумайте про те, щоб перейти в іншу кімнату і зачинити двері або сісти якомога далі від інших.

Розумні пристрої з голосовим управлінням завжди слухають і можуть надсилати звукові записи на свої хмарні сервери. Намагайтеся уникати роботи поблизу цих пристроїв або вимикайте їх під час розмов.

Змініть назву домашньої мережі **Wi-Fi за замовчуванням** та **пароль інтернет-маршрутизатора** за замовчуванням (паролі за замовчуванням доступні в Інтернеті для хакерів). Використовуйте надійний пароль із цифрами, літерами та символами.



Працюйте безпечно в дорозі

Будьте обережні, щоб не втратити пристрої, документи або інформацію про клієнтів KPMG або не наразити їх на ризик крадіжки, коли ви перебуваєте поза межами офісу:

- Ніколи не залишайте пристрої або документи (включаючи блокноти та інші записи зустрічей) **без нагляду в громадських місцях** - завжди тримайте їх при собі.
- Ніколи не залишайте пристрої **без нагляду в автомобілі,** особливо на ніч.
- Завжди **повністю вимикайте ноутбук** перед тим, як перевозити його з одного місця в інше. Якщо він буде загублений або викрадений, зловмиснику буде важче отримати доступ до нього, якщо він буде повністю вимкнений.
- Якщо ваша Фірма-член надає **екрани конфіденційності для ноутбуків**, завжди використовуйте їх, щоб не дозволити стороннім особам переглядати інформацію на вашому екрані.
- Не дозволяйте стороннім людям **підслуховувати вас,** , коли ви обговорюєте конфіденційну інформацію - перейдіть у приватну зону/кімнату.
- Переконайтеся, що ви використовуєте **безпечне VPN-з'єднання,** якщо вам потрібно користуватися громадським Wi-Fi для доступу до Інтернету з ноутбука KPMG. Громадський Wi-Fi є незахищеним, і ви можете бути вразливими до атак.
- Вимикайте **Bluetooth** на вашому мобільному пристрої, якщо це не потрібно, і не приймайте неініційовані запити на сполучення від інших пристроїв для запобігання доступу зловмисників до вашого пристрою.

Перш ніж вирушати у міжнародну ділову поїздку, усвідомте, що інформація та пристрої, якими ви володієте, можуть бути піддані більшому **ризику втрати, крадіжки або навіть шпигунства**, що може призвести до потенційного розголошення інформації. Якщо ви вважаєте, що ваш пункт призначення пов'язаний з вищим, ніж зазвичай, ризиком, подумайте про вжиття додаткових заходів безпеки перед виїздом і під час подорожі. Мінімізуйте кількість інформації, яку ви берете з собою, і подумайте про те, щоб подорожувати з **"чистим" ноутбуком**.

Завжди, коли це можливо, тримайте при собі **мобільний пристрій, ноутбук, планшет** і будь-яке інше обладнання або документи.

Працюйте безпечно в приміщеннях KPMG

Безпека в приміщеннях KPMG - це відповідальність кожного, тому, будь ласка, допомагайте підтримувати безпечне та захищене робоче середовище.

Підтримуйте безпечний робочий простір

Підтримання **чистоти та конфіденційності робочого місця** (наприклад, робочого столу, кімнати для переговорів, тихої кімнати) допомагає уникнути втрати та крадіжки інформації, а також надає клієнтам та гостям впевненості в тому, що KPMG захищає інформацію належним чином.

Конфіденційні зустрічі або бесіди

- Уникайте відкритого обговорення **конфіденційної або комерційно важливої інформації** (наприклад, в офісі з відкритим плануванням або в ліфті).
- Наприкінці зустрічі переконайтеся, що вся **інформація на дошках** стерта, а **фліпчарти** чи **нотатки** ви забрали з собою або надійно утилізували.

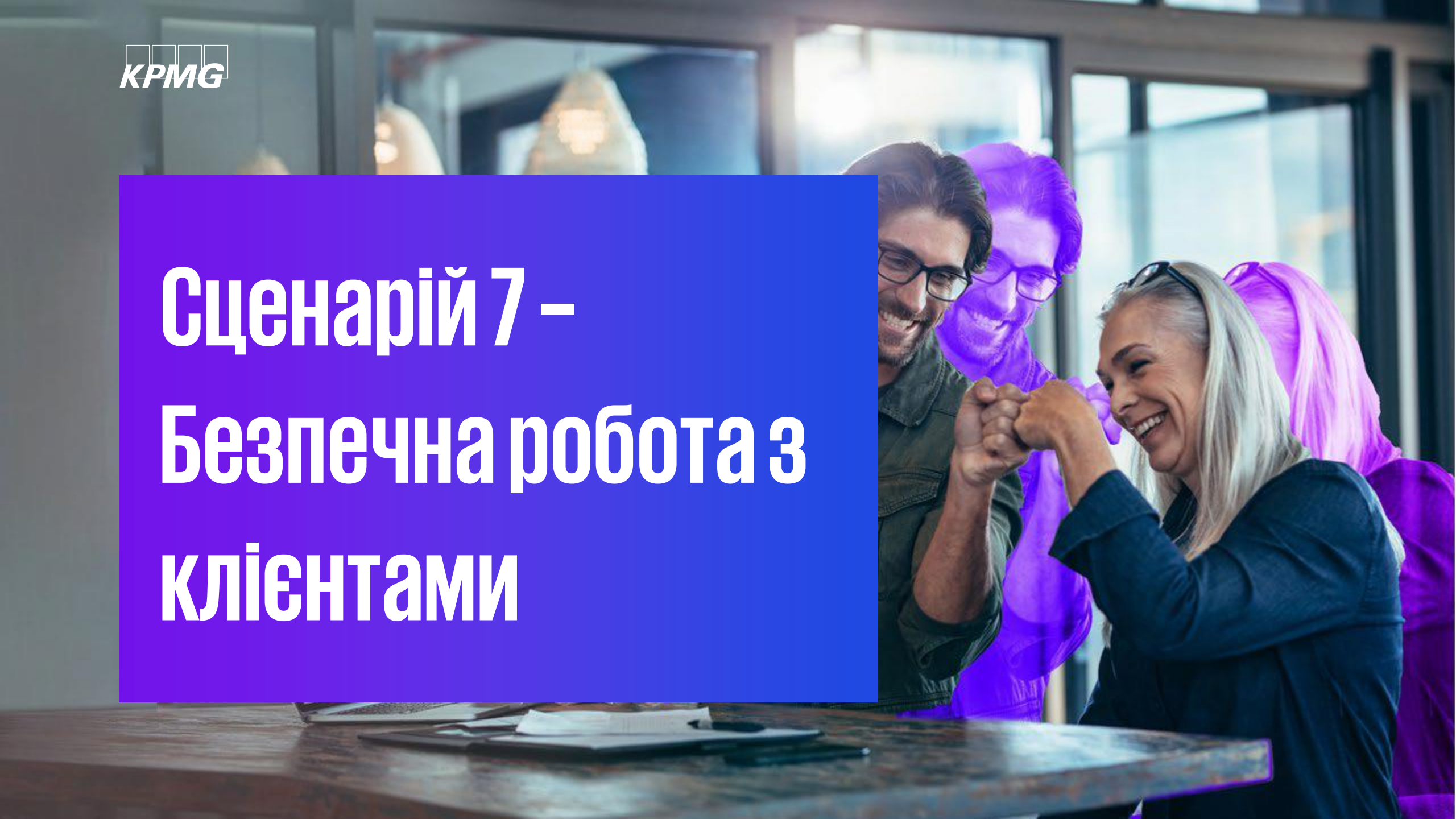
Документи

- Негайно забирайте всі **друковані матеріали**.
- Утилізуйте непотрібні конфіденційні документи у спеціальному **контейнері для безпечної утилізації**.

Ноутбуки

- За можливості, фіксуйте свій ноутбук за допомогою **тросового замка**.
- Використовуйте **екран конфіденційності** (якщо він є), щоб інформацію не могли прочитати перехожі.
- Ніколи не записуйте свої **паролі**.
- Завжди блокуйте **екран ноутбука,** коли ви залишаєте його без нагляду. Натисніть "Ctrl_Alt_Del", а потім "Enter" (або клавішу Windows і клавішу "L").
- Залишаючи робоче місце на цілий день, візьміть ноутбук із собою або переконайтеся, що він **замкнений** у шафі чи безпечному місці.

Захищайте свій офіс (і колег) від непроханих гостей - Якщо хтось без бейджа намагається увійти до офісу, коли ви заходите або виходите, **не впускайте його.** Попросіть в такої особи пояснення і супроводжуйте її до стійки реєстрації, якщо це буде необхідно. Перебуваючи в приміщеннях KPMG, **завжди показуйте свій бейдж** , щоб продемонструвати, що ви маєте право доступу, і знімайте його, коли виходите з приміщення.



Сценарій 7 – Безпечна робота з клієнтами

Сценарій 7 – Безпечна робота з клієнтами

Габріель та Єва щойно виграли новий проєкт для великого постачальника медичних послуг. Тепер вони повинні забезпечити безпечне управління всіма ризиками в проєкті. Що вони можуть зробити, щоб гарантувати безпечну співпрацю з клієнтом?

Які з цих кроків ви повинні зробити, щоб безпечно працювати з клієнтами?

Винесення даних клієнта з офісу клієнта без попереднього дозволу

Перевірка вимог клієнта щодо підключення до його мережі

Якщо клієнт потребує винятку з політики, зверніться до Національного спеціаліста з IT-безпеки

Дотримуйтесь відповідних політик клієнта та KPMG

Залишайте пристрої KPMG без нагляду в приміщенні клієнта

Слід дотримуватись лише політик KPMG, а не клієнта

Відповідь:

ТАК

Перевірка вимог клієнта щодо підключення до його мережі

Якщо клієнт потребує винятку з політики, зверніться до Національного спеціаліста з IT-безпеки

Дотримуйтесь відповідних політик клієнта та KPMG

НІ

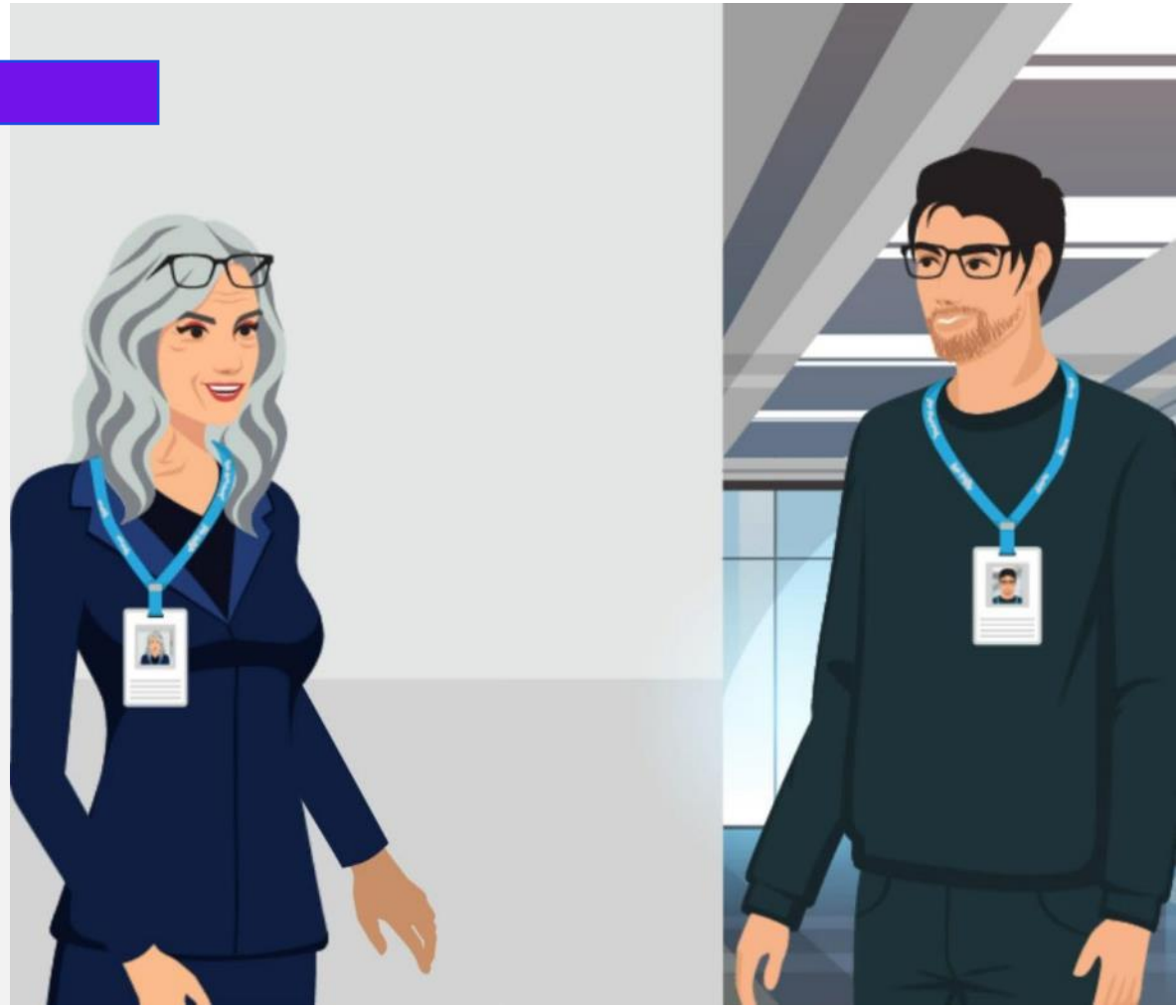
Винесення даних клієнта з офісу клієнта без попереднього дозволу

Залишайте пристрої KPMG без нагляду в приміщенні клієнта

Слід дотримуватись лише політик KPMG, а не клієнта

Сценарій 7 – Безпечна робота з клієнтами

Клієнт просить команду створити додаток, який буде зберігати конфіденційні персональні дані про стан здоров'я пацієнтів у хмарному середовищі. Габріель має великий досвід у цій сфері і хоче негайно почати роботу. Але його цікавить, чи не потрібно буде в якийсь момент, зважаючи на конфіденційність даних, проводити оцінку ризиків? Коли Габріелю слід ініціювати оцінку ризиків рішення?



Сценарій 7 – Безпечна робота з клієнтами

Коли Габріелю слід ініціювати оцінку ризиків рішення?

A. Йому слід зробити це після того, як рішення буде створено, щоб група оцінювання могла дослідити повну функціональність інструменту.

B. Йому слід ініціювати цей процес зараз, до того, як почати будь-яку роботу з рішенням.

Сценарій 7 – Безпечна робота з клієнтами

Коли Габріелю слід ініціювати оцінку ризиків рішення?

A. Йому слід зробити це після того, як рішення буде створено, щоб група оцінювання могла дослідити повну функціональність інструменту.

B. Йому слід ініціювати цей процес зараз, до того, як почати будь-яку роботу з рішенням.

Сценарій 7 – Безпечна робота з клієнтами

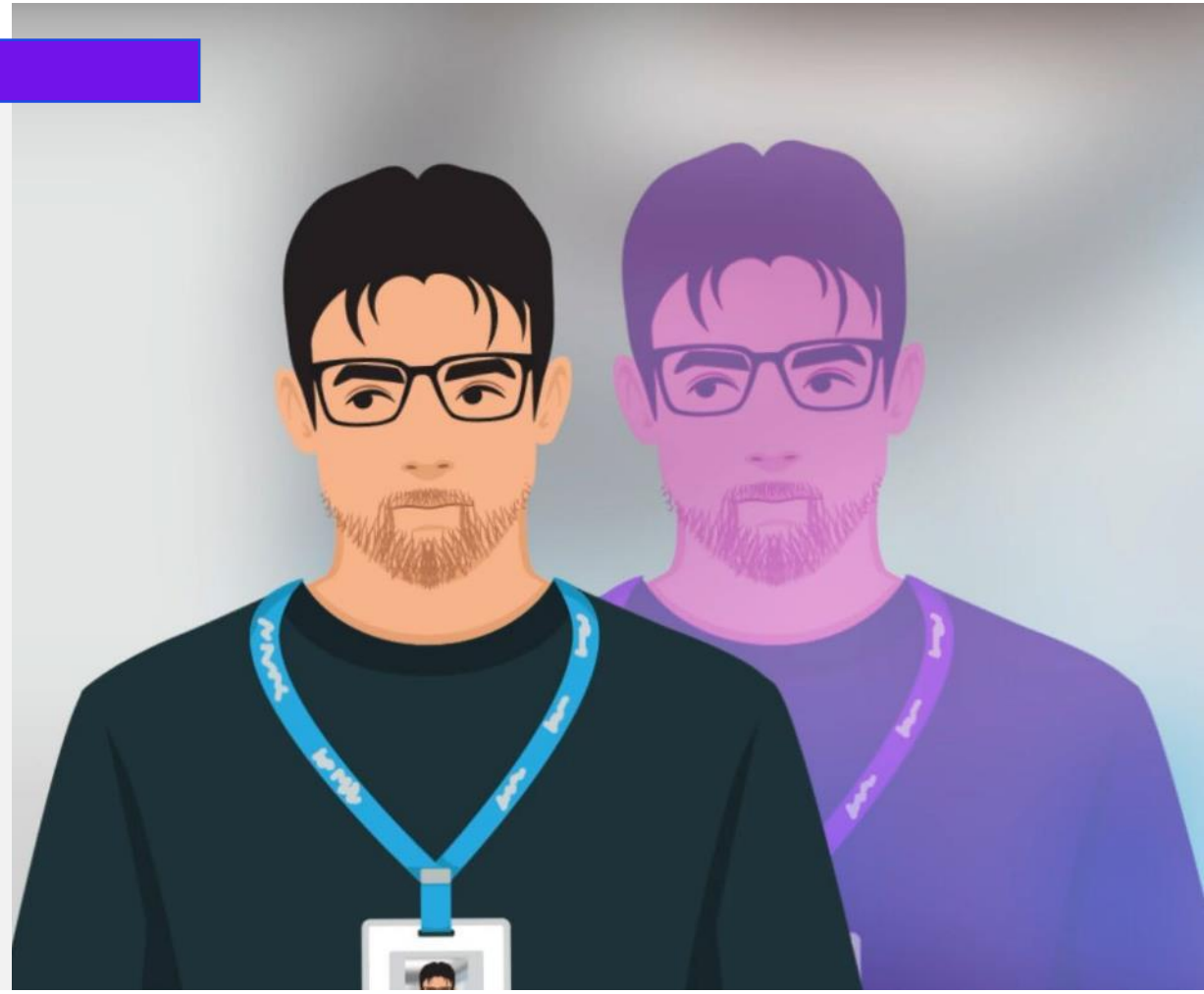
Важливо впевнитися в тому, що **всі** проєкти, пов'язані з даними KPMG або клієнтів, проходять перевірку на предмет інформаційних ризиків і ризиків порушення конфіденційності якомога раніше, оскільки це дозволяє фірмі проаналізувати, виявити і мінімізувати ризики проєкту або ініціативи ще до початку вашої роботи над ним, а також запровадити необхідні засоби контролю безпеки та конфіденційності.

Необхідно також вжити запобіжних заходів для захисту персональних і конфіденційних персональних даних від втрати або несанкціонованого розголошення. Вони повинні включати відповідні технічні, фізичні та організаційні заходи безпеки відповідно до рівня конфіденційності інформації та рівня ризику, пов'язаного з обробкою (наприклад, захист доступу до облікового запису за допомогою суворих вимог до паролів та багатофакторної автентифікації).

! Дотримуйтесь процесу оцінки ризиків у вашій Фірмі-члені (наприклад, консультуйтеся з службою ITS або Національним спеціалістом з IT-безпеки (NITSO)) щодо всіх проєктів та ініціатив, де задіяні дані або IT-активи, або де проєкти можуть спричинити ризик для інформації або конфіденційності.

Сценарій 7 – Безпечна робота з клієнтами

Габріель вирішує зв'язатися з відділом оцінки ризиків зараз, перед початком будь-яких робіт. Він хоче переконатися, що всі вимоги технічної безпеки будуть враховані в проєкті з самого початку. Через кілька тижнів Габріель і Єва зустрічаються з клієнтом в його офісі. Клієнт показує їм набір даних, які він планує надати, але Єва помічає, що він містить більше даних про пацієнтів, ніж необхідно для досягнення мети проєкту. Як Єва повинна відповісти клієнту?



Сценарій 7 – Безпечна робота з клієнтами

Що Єва повинна відповісти клієнту?

A. Вона повинна попросити клієнта відредагувати набір даних, щоб видалити непотрібні стовпці, перш ніж він надасть його.

B. Їй слід прийняти набір даних з додатковими стовпчиками, оскільки ця інформація може стати в нагоді на подальших етапах проєкту. Крім того, клієнти можуть образитися, якщо ви поставите під сумнів дані, які вони надають для власного проєкту.

Сценарій 7 – Безпечна робота з клієнтами

Що Єва повинна відповісти клієнту?

A. Вона повинна попросити клієнта відредагувати набір даних, щоб видалити непотрібні стовпці, перш ніж він надасть його.

B. Їй слід прийняти набір даних з додатковими стовпчиками, оскільки ця інформація може стати в нагоді на подальших етапах проєкту. Крім того, клієнти можуть образитися, якщо ви поставите під сумнів дані, які вони надають для власного проєкту.

Сценарій 7 – Безпечна робота з клієнтами

Якщо ви працюєте з персональними або конфіденційними персональними даними, важливо не приймати більше інформації, ніж це необхідно для мети, для якої вона початково збиралася. Це частина Принципів конфіденційності даних KPMG, які гарантують дотримання нами законодавства про конфіденційність даних.

Якщо клієнт надає більше інформації, ніж необхідно для цілей вашого завдання, повідомте про це менеджера або керівника проєкту, який може обговорити це питання з клієнтом.

Сценарій 7 – Безпечна робота з клієнтами

Єва дякує клієнту, але припускає, що з огляду на закони про захист даних, було б краще взяти лише те, що необхідно для виконання умов договору про надання послуг. Клієнт погоджується, що це правильний спосіб дій, і дякує Єві за те, що вона нагадала йому про закони про захист даних.

Сценарій 7 – Безпечна робота з клієнтами

У цьому сценарії ви дізналися про управління ризиками проєкту під час роботи з клієнтами, включаючи таке:
- безпечна робота в офісі клієнта,
- дотримання положень плану захисту інформації для проєкту,
- забезпечення того, щоб усі необхідні аспекти взаємодії пройшли оцінку ризиків на початку проєкту,
- дотримання правил конфіденційності даних, наприклад, не збирати більше даних від клієнта, ніж це необхідно для виконання завдання.

Щоб дізнатися більше, оберіть КЛЮЧОВІ МІРКУВАННЯ.

Запити та анкети клієнтів

Клієнти, потенційні клієнти, постачальники, регуляторні органи та інші зацікавлені сторони часто запитують фірми, що входять до складу KPMG, про наші **політики, процедури та засоби контролю** захисту конфіденційної інформації.

Типові запитання та запити на інформацію включають таке

Чи має KPMG **політики інформаційної безпеки?**

Яким чином KPMG **захищає дані,** які ми отримуємо?

Чи має KPMG **плани безперервності діяльності та аварійного відновлення**?

Чи надаємо ми копії текстів наших **політик**?

Чи проводить KPMG тренінги із захисту інформації та конфіденційності ?

Чи має KPMG **сертифікат ISO 27001**?

Чи можуть наші клієнти **проводити аудит** наших засобів контролю безпеки та конфіденційності та/або проводити **тест на проникнення** в наші системи та мережу?

Якщо ви отримали запит або анкету від клієнта

Негайно зв’яжіться з Національним керівником з IT-безпеки (NITSO) KPMG.

Він буде виконувати роль основної контактної особи для відповіді клієнтам або іншим зацікавленим сторонам щодо практик інформаційної безпеки KPMG.

Конфіденційна персональна інформація

KPMG зберігає персональні дані про людей, включаючи співробітників, підрядників, клієнтів або співробітників клієнтів. Ми також обробляємо великі обсяги персональних даних від імені клієнтів.

Персональні дані - це будь-яка інформація про фізичну особу, яка може бути використана окремо чи у сукупності з іншою інформацією для ідентифікації конкретної фізичної особи.

Приклади:

- Повне ім'я
- Адреса
- Дата народження
- Електронна адреса
- Номер телефону
- Ідентифікаційний номер
- Голос або зображення особи, що містяться в аудіо- та відеозаписах

До конфіденційних персональних даних можуть належати персональні дані, які розкривають про особу таку інформацію:

Приклади:

- Раса або етнічна приналежність
- Політичні переконання
- Релігійні або філософські погляди
- Кримінальне минуле
- Членство в профспілках
- Інформація про стан здоров'я
- Сексуальна орієнтація
- Біометрична або генетична інформація

Конфіденційні персональні дані, ймовірно, мають приватний характер і **можуть бути використані в дискримінаційний спосіб**, тому з ними потрібно поводитися ще більш обережно, ніж з персональними даними. Для обробки конфіденційних персональних даних, як правило, потрібна пряма згода відповідних фізичних осіб.

Безпечна робота в офісах клієнтів

Захищайте пристрої та документи KPMG, вивезені за межі офісу, так само, як це було б зроблено в приміщеннях KPMG

- Ніколи не залишайте **пристрої KPMG (ноутбуки та мобільні телефони)** без нагляду. Якщо можливо, використовуйте захисний тросовий замок (прикріплений до нерухомої точки фіксації), щоб захистити свій ноутбук, якщо на території клієнта у вас немає доступу до сховища, що замикається.
- Завжди **блокуйте екран ноутбука,** коли ви залишаєте його без нагляду. Натисніть "Ctrl_Alt_Del", а потім "Enter" (або клавішу Windows і клавішу "L").
- Якщо ви працюєте з конфіденційною інформацією на ноутбуці, використовуйте **екран конфіденційності** (якщо він є).
- Якщо ви залишаєте сумки для ноутбуків чи інші сумки без нагляду, переконайтеся, що в них немає **пристроїв або конфіденційної інформації KPMG чи клієнтів**.
- Не залишайте **документи** без нагляду - за можливості замикайте їх у безпечній шухляді стола або в шафі.
- Не обробляйте інформацію KPMG, **яка не має відношення до завдання клієнта,** перебуваючи на об'єктах клієнта, за винятком випадків, коли це є абсолютно необхідним.
- Не вилучайте будь-яку **надану клієнтом документацію** чи **знімні електронні носії** з об'єкта клієнта без його дозволу та погодження з менеджером проєкту.
- Утилізуйте всі **конфіденційні відходи** в контейнерах для конфіденційних відходів Клієнта.
- Пам'ятайте, що ви можете бути зобов'язані дотримуватися положень **політики інформаційної безпеки клієнта**, а також політики інформаційної безпеки KPMG.

Підключення до мережі клієнта

Якщо ви працюєте в офісі клієнта, вам, швидше за все, **знадобиться доступ до мережі клієнта** або доступ до систем KPMG через інтернет-з'єднання клієнта. Щоб забезпечити безпеку та цілісність IT-систем KPMG та клієнта, ознайомтеся з цими рекомендаціями *перед підключенням*:

Дотримуйтесь усіх належних політик KPMG

Отримайте **письмовий дозвіл** клієнта та партнера проєкту на доступ до мережі клієнта. Зверніться до свого підрозділу ITS за допомогою щодо будь-яких технічних вимог або вимог безпеки.

(Хоча вам зазвичай не потрібен письмовий дозвіл на підключення до **гостьового Wi-Fi**, можливо, вам доведеться підписати заяву про прийнятне використання).

Зверніться до IT-департаменту клієнта

Щоб відповідати будь-яким вимогам безпеки, технічним або процедурним вимогам, проконсультуйтеся з **IT-департаментом клієнта**. Якщо клієнт попросить вас внести зміни у ваш ноутбук або інше обладнання, видане KPMG, перш ніж це зробити, зверніться до свого відділу ITS.

Дотримуйтесь політик безпеки та використання IT клієнта

Дотримуйтесь положень політик **KPMG та клієнтів** з питань використання їхніх мереж та систем. Наприклад, клієнт може не дозволити використовувати свої ресурси в особистих цілях. Так само він, швидше за все, не захоче, щоб його ресурси використовувалися для роботи, пов'язаної з іншими клієнтами KPMG.

Не припускайте, що будь-які два клієнти мають однакові вимоги до підключення до їхніх мереж.

Будь-яке пошкодження або втрата даних внаслідок недотримання вами правил KPMG або клієнтів може призвести до порушення конфіденційності, нанесення шкоди репутації, втрати завдань або судового позову проти KPMG.

Підключення співробітників клієнтів до мереж KPMG

Якщо клієнту необхідно буде підключитися до мережі KPMG у процесі співпраці з вами, **подайте запит** Національному спеціалісту з IT-безпеки (NITSO). Після того, як NITSO розгляне та схвалить запит, переконайтеся, **що відповідні процедури** були дотримані, включаючи (де це можливо), забезпечте, щоб клієнти підключали свої пристрої через гостьову мережу Wi-Fi.

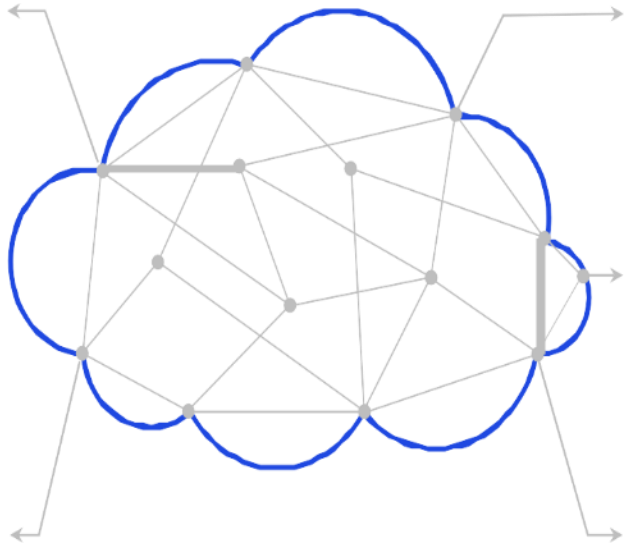
Використання безпечних хмарних сервісів

Остерігайтеся використовувати **несанкціоновані публічні хмарні сервіси** для зберігання або передачі інформації.

Такі популярні сервіси, як **Gmail, Dropbox, Siri, Google Translate та інструменти генеративного ШІ,** можуть бути корисними, але вони не дозволені (за винятком випадків, коли місцевий NITSO попередньо затвердив виняток) для обробки, зберігання або обміну інформацією про фірми-члени KPMG або клієнтів з кількох причин.

Ризики використання несанкціонованих хмарних сервісів включають такі

01 Конфіденційна інформація/дані про клієнтів KPMG або фірм-членів можуть стати **надбанням громадськості** внаслідок компрометації сервісу.



02 Дані можуть **залишитися** на сервісі після їх знищення вами, що, в свою чергу, може порушити політики зберігання даних наших фірм-членів

03 Дані можуть бути **збережені** без належного їх відокремлення від даних інших користувачів, що допускає можливість випадкового або зловмисного розголошення третім особам

04 Персональна інформація може **передаватися** через кордони, що може викликати порушення Політики конфіденційності KPMG або місцевих законів

05 Працівники сервісу можуть **бачити** і копіювати завантажені вами дані

Якщо клієнт попросить використовувати **несанкціонований хмарний сервіс** для обміну файлами під час виконання завдання, Партнер проєкту повинен буде спочатку проконсультуватися з підрозділом управління якістю та ризиками.

Несанкціоновані хмарні сервіси можуть бути авторизовані **Національним спеціалістом з питань IT-безпеки і Партнером з управління ризиками** після офіційної оцінки ризиків.

Оцінка ризиків порушення безпеки та конфіденційності в рамках проєктів

Важливо впевнитися в тому, що всі проєкти, пов'язані з даними KPMG або клієнтів, **проходять перевірку на предмет інформаційних ризиків і ризиків для конфіденційності** якомога раніше, оскільки це дозволяє фірмі проаналізувати, виявити і мінімізувати ризики проєкту або ініціативи ще до початку вашої роботи над ним.

Це дозволяє нам **зрозуміти існуючу систему або середовище,** аналізуючи відповідну інформацію (наприклад, додатки, мережеву архітектуру, бізнес-процеси тощо), або зрозуміти більше **дані, що обробляються**.

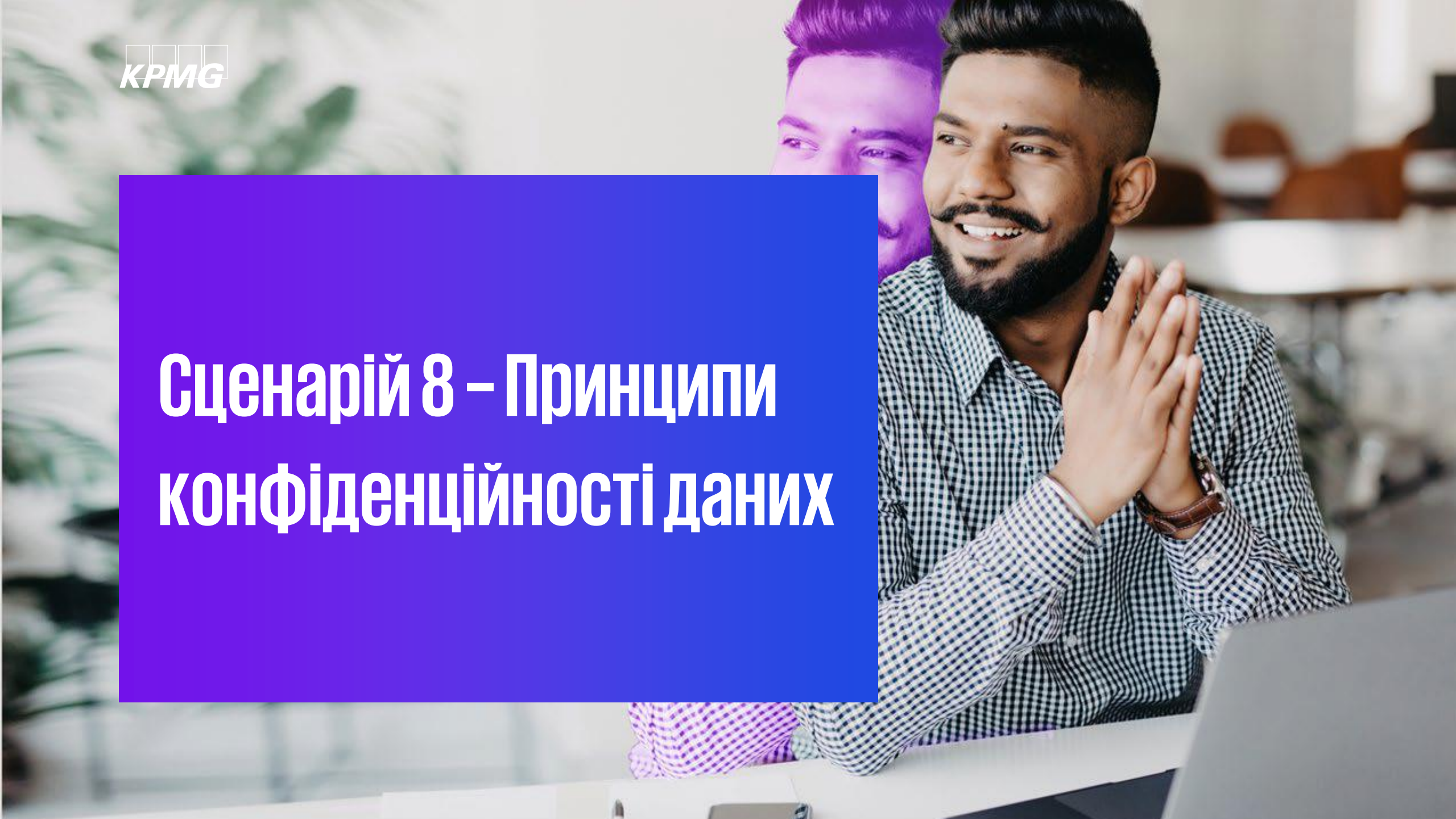
Ініціювання цього процесу **на ранньому етапі проєкту** дозволяє нам запровадити необхідні засоби контролю безпеки.

Дотримуйтесь процесу оцінки ризиків у вашій Фірмі-члені **Фірмі-члені** щодо всіх проєктів та ініціатив, де задіяні дані або IT-активи, або де проєкти можуть спричинити ризик для інформації. Такі проєкти можуть включати:

- **Нові IT-системи та мережі,** які підтримують бізнес-процеси та дані, наприклад, хмарні інвестиційні рішення, генеративний ШІ
- **Суттєві зміни в бізнесі** (наприклад, злиття, поглинання або продаж)
- **Нові бізнес-процеси**
- **Бізнес-додатки**
- **Нове приміщення KPMG**
- **проєкти,** пов’язані з обробкою **конфіденційних персональних даних**

Якщо ви хочете дізнатися більше про оцінку ризиків для інформації та конфіденційності, зверніться до вашого місцевого Національного спеціаліста з IT-безпеки (NITSO) та/або представників підрозділу забезпечення якості та управління ризиками.

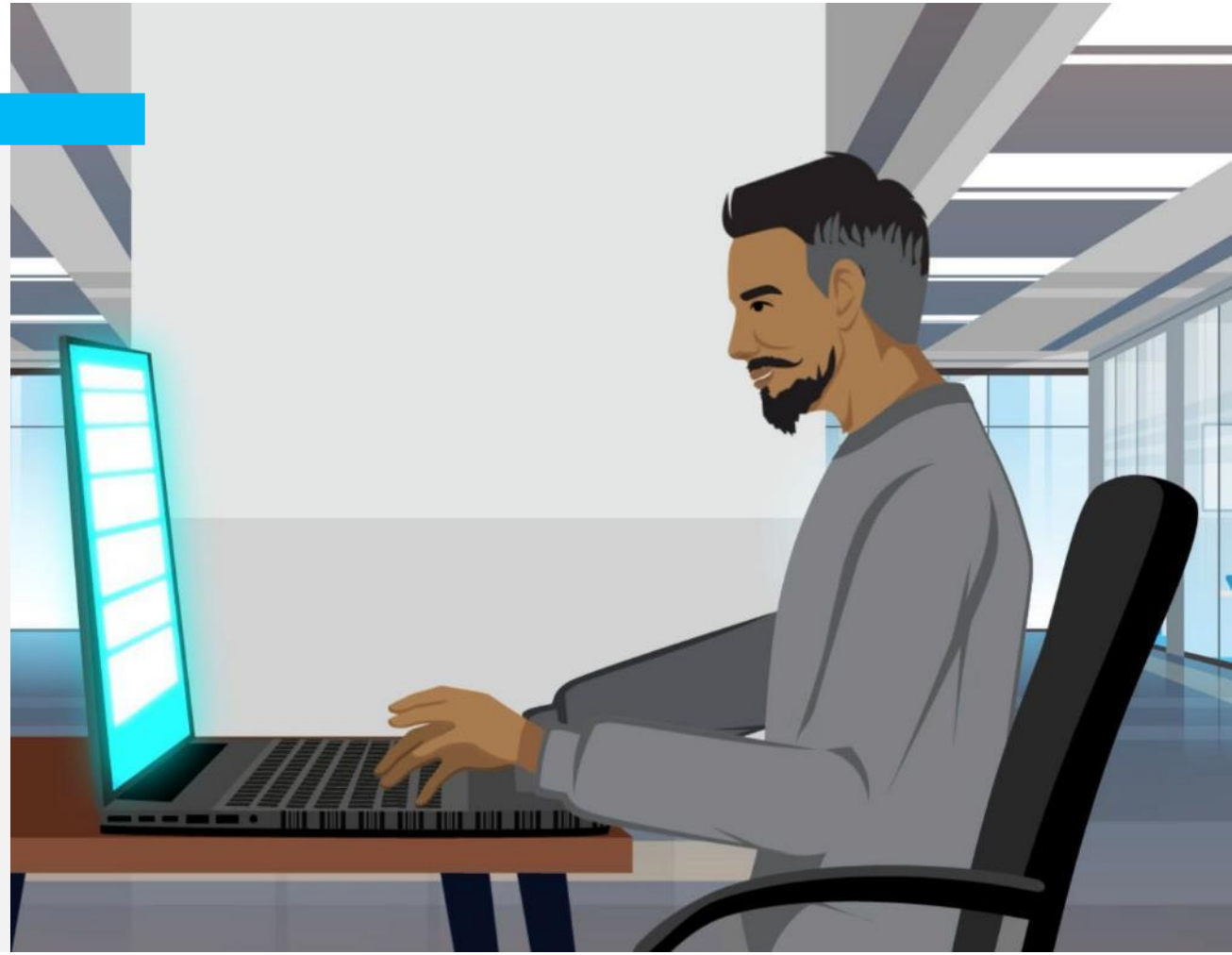
Запити на винятки з політики - Якщо ви отримаєте запит від клієнта під час виконання завдання, наприклад, щодо використання/встановлення несанкціонованого програмного забезпечення на пристрої KPMG, проконсультуйтеся з керівником проєкту, який розгляне та оцінить запит спільно з Національним спеціалістом з IT-безпеки (NITSO) та Партнером з управління ризиками.



Сценарій 8 – Принципи конфіденційності даних

Сценарій 8 – Принципи конфіденційності даних

Сохейл - менеджер, який працює в підрозділі корпоративного оподаткування. Він консультує клієнта щодо винагород працівникам, і, оскільки це пов'язано з обробкою їхніх персональних даних, він хоче дізнатися більше про принципи конфіденційності даних в KPMG.



10 Принципів конфіденційності даних

1. **Прозорість** - Фірми KPMG нададуть особам інформацію про те, як ми обробляємо їх персональні дані в обсязі, необхідному для забезпечення чесності обробки.

2. **Обмеження цілі** – Фірми KPMG обробляють Персональні дані тільки для досягнення таких цілей:
   - цілі, викладені в будь-якому повідомленні, що надається відповідним особам, які мають відношення до KPMG,
   - коли це вимагається законом, або
   - у випадку наявності згоди відповідних осіб.

3. **Якість та пропорційність даних** - Персональні дані повинні бути точними та, за потреби, актуальними. Персональні дані, якими володіють фірми KPMG, повинні бути достатніми, релевантними та не надмірними для цілей, для яких вони передаються між фірмами KPMG, а також повинні зберігатися лише стільки часу, скільки необхідно для цілей відповідної обробки.

4. **Безпека та конфіденційність** - Необхідно вживати розумних запобіжних заходів для захисту персональних даних від випадкового або незаконного знищення або втрати, зміни, несанкціонованого розкриття або доступу. Для дотримання місцевих звичаїв, законів або нормативних актів можуть знадобитися додаткові заходи.

5. **Доступ, виправлення, видалення та заперечення** – Фізичні особи повинні мати доступ до своїх персональних даних, якщо їхні запити є обґрунтованими та дозволеними законом. Фізична особа може заперечити проти обробки за наявності вагомих законних підстав, і KPMG виправить, змінить або видалить персональні дані за необхідності.

10 Принципів конфіденційності даних

6 **Конфіденційні дані** - У випадках, коли фірми KPMG обробляють конфіденційні персональні дані, вони вживають таких додаткових заходів (наприклад, пов'язаних з безпекою), які необхідні для захисту таких конфіденційних персональних даних відповідно до чинного законодавства.

7 **Дані, що використовуються в маркетингових цілях** - У випадках, коли фірми KPMG обробляють персональну інформацію для цілей прямого маркетингу, такі фірми KPMG повинні мати ефективні процедури, що дозволяють фізичним особам у будь-який час відмовитися від використання їхньої персональної інформації для таких цілей.

8 **Автоматизована обробка** - У випадках, коли фірми KPMG обробляють персональну інформацію виключно в автоматизованому режимі, що має значний вплив на особу, такі фірми KPMG надають особі можливість обговорити результати такої обробки перед прийняттям рішення (за винятком випадків, коли інше дозволено чинним законодавством).

9 **Мінімізація даних** - У випадках, коли фірми KPMG зберігають персональну інформацію фізичної особи, ці фірми KPMG зберігають її у формі, що дозволяє ідентифікувати особу, лише доти, доки вона слугує цілі (цілям), для яких вона була спочатку зібрана або згодом дозволена, за винятком випадків, дозволених чинним законодавством.

10 **Передача інформації та дотримання вимог** – У межах глобальної мережі фірм KPMG персональні дані можуть передаватися за межі країни, в якій вони були зібрані, для здійснення законної господарської діяльності відповідно до чинного законодавства

Сценарій 8 – Принципи конфіденційності даних

Одного дня він отримує електронного листа від співробітника свого клієнта. Цей працівник незадоволений тим, що KPMG обробляє особисту інформацію про нього під час виконання завдання, і хотів би дізнатися більше інформації про це. Що слід зробити Сохейлу у відповідь на цю скаргу?

Сценарій 8 – Принципи конфіденційності даних

Що Сохейл має зробити щодо цієї скарги?

A. Він повинен негайно повідомити про це свого керівника проєкту, щоб останній міг оперативно вирішити питання.

B. Він повинен негайно проінформувати клієнта. Це співробітник клієнта, тому цю скаргу має розглядати клієнт, а не KPMG.

Сценарій 8 – Принципи конфіденційності даних

Що Сохейл має зробити щодо цієї скарги?

A. Він повинен негайно повідомити про це свого керівника проєкту, щоб останній міг оперативно вирішити питання.

B. Він повинен негайно проінформувати клієнта. Це співробітник клієнта, тому цю скаргу має розглядати клієнт, а не KPMG.

Сценарій 8 – Принципи конфіденційності даних

Таким чином керівник проєкту може зв'язатися з місцевим спеціалістом з питань конфіденційності (PL), який зможе проконсультувати щодо відповідних наступних кроків.

Ми зобов'язані відповідати на такі типи запитів, коли ми обробляємо персональні дані особи в рамках виконання завдання.

Сценарій 8 – Принципи конфіденційності даних

Сохейл вирішує негайно повідомити про скаргу свого керівника проєкту, оскільки KPMG зобов'язана відповідати на подібні запити протягом певного часу. Пізніше Сохейл отримує ще одного електронного листа - цього разу від постачальника, який повідомляє, що вони переносять місце зберігання хмарних даних з Німеччини до Чилі. Він розуміє, що це вплине на його роботу, оскільки персональні дані зберігаються в цьому хмарному рішенні. Що Сохейлу слід робити далі?

Сценарій 8 – Принципи конфіденційності даних

Що Сохейл має робити далі?

A. Йому слід сказати постачальнику, щоб він продовжував роботу, оскільки послуга, яку надає постачальник, є життєво важливою для обробки даних в рамках цього завдання, тож вона має надаватися без перебоїв.

B. Він повинен проконсультуватися зі Спеціалістом з питань конфіденційності (PL), щоб визначити, чи буде ця зміна відповідати будь-яким застосовним регуляторним вимогам щодо конфіденційності даних, а також додатковим вимогам щодо конфіденційності (якщо такі є), узгодженим з клієнтом в умовах договору про виконання завдання.

Сценарій 8 – Принципи конфіденційності даних

Що Сохейл має робити далі?

A. Йому слід сказати постачальнику, щоб він продовжував роботу, оскільки послуга, яку надає постачальник, є життєво важливою для обробки даних в рамках цього завдання, тож вона має надаватися без перебоїв.

B. Він повинен проконсультуватися зі Спеціалістом з питань конфіденційності (PL), щоб визначити, чи буде ця зміна відповідати будь-яким застосовним регуляторним вимогам щодо конфіденційності даних, а також додатковим вимогам щодо конфіденційності (якщо такі є), узгодженим з клієнтом в умовах договору про виконання завдання.

Сценарій 8 – Принципи конфіденційності даних

Перенесення обробки персональних даних в іншу країну (у тому числі за межі Європейської економічної зони (ЄЕЗ)) може спричинити потребу виконувати додаткові вимоги щодо конфіденційності даних, яким має відповідати KPMG.

Сохейлу слід проконсультуватися зі Спеціалістом з питань конфіденційності (PL), щоб KPMG розуміла наслідки переміщення даних, що може включати оцінку наслідків передачі.

У разі виникнення сумнівів звертайтеся до місцевого Спеціаліста з питань конфіденційності (PL) за додатковими рекомендаціями щодо міжнародної передачі даних, включаючи передачі даних між Фірмами-членами.

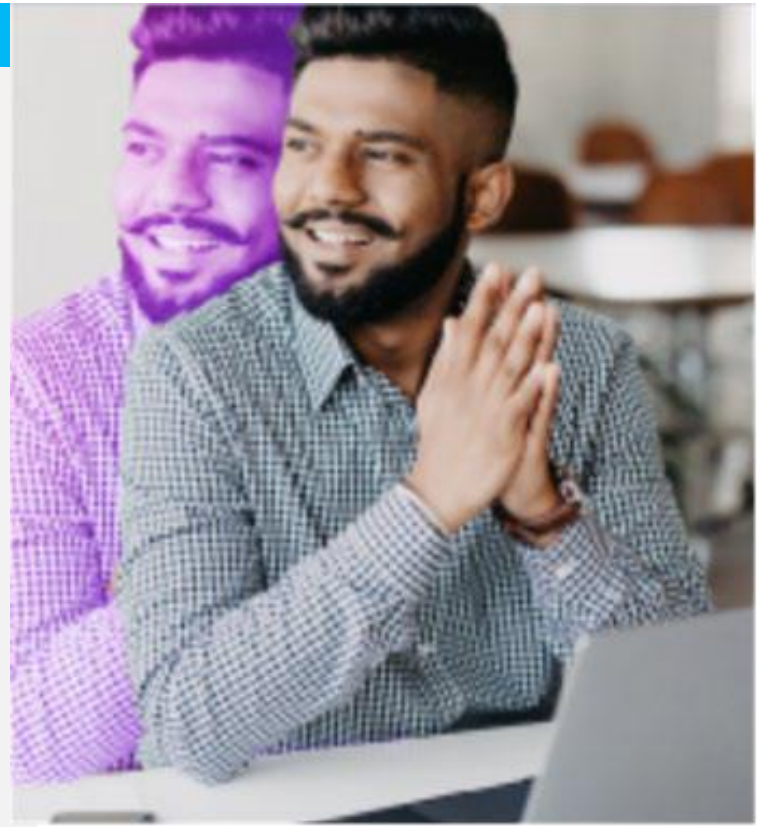
Сценарій 8 – Принципи конфіденційності даних

Перш ніж відповісти постачальнику, Сохейл негайно консультується зі спеціалістом з питань конфіденційності, щоб KPMG розуміла наслідки переміщення даних (що може включати оцінку впливу на передачу).

Сценарій 8 – Принципи конфіденційності даних

У цьому сценарії ви дізналися про таке:
- Принципи конфіденційності даних,
- скарги від фізичних осіб щодо обробки фірмою KPMG їхніх приватних даних, а також
- міркування щодо міжнародної передачі даних.

Щоб дізнатися більше, оберіть КЛЮЧОВІ МІРКУВАННЯ.



Принципи конфіденційності даних

KPMG дотримується 10 Принципів конфіденційності даних, щоб допомогти нам дотримуватися законодавства про конфіденційність даних

Ці принципи поширюються на **всіх співробітників KPMG,** які мають доступ до персональної інформації, включаючи вас.

Ці принципи **поділяють і дотримуються їх у своїй роботі** всі фірми-члени KPMG.

Принципи конфіденційності даних надають **загальну основу,** яка допомагає нам краще обслуговувати наших клієнтів, колег і наші громади.

Ви можете знайти більше інформації про Принципи конфіденційності даних у **"Глобальній політиці конфіденційності"** (див. "Ресурси").

1. Прозорість
2. Обмеження цілей
3. Якість та пропорційність даних
4. Безпека та конфіденційність
5. Доступ, виправлення, видалення та заперечення
6. Конфіденційні дані
7. Дані, що використовуються для маркетингових цілей
8. Автоматизована обробка
9. Мінімізація даних
10. Передача інформації та дотримання вимог

Розпорядник (володілець) даних і обробник даних

Однією з особливостей законодавства про конфіденційність даних є різні ролі розпорядників даних і обробників даних

Обидва повинні дотримуватися законів про конфіденційність, але їхні обов'язки відрізняються:

Розпорядники даних вирішують, з якою метою та яким способом обробляються персональні дані.

Обробники даних обробляють персональні дані від імені розпорядника даних.

По відношенню до **даних KPMG**, фірма KPMG виступає в якості розпорядника і дотримується 10 принципів конфіденційності даних.

По відношенню до **даних клієнта**, у нашому договорі буде зазначено, ким виступатиме KPMG - розпорядником даних чи обробником даних.

Обробка означає будь-яку операцію або набір операцій, яка чи які виконуються з персональними даними або наборами персональних даних за допомогою автоматизованих засобів чи ні, включаючи таке:

- збір
- запис
- організація
- структурування
- зберігання
- адаптація або зміна
- збереження
- консультування
- використання
- розкриття шляхом передачі
- розповсюдження або надання доступу іншим чином
- узгодження або комбінування
- обмеження
- стирання або знищення

Запити суб'єктів даних на доступ (DSARs)

Запит суб'єкта даних (DSAR) на доступ - це запит фізичної особи на доступ до інформації про її персональні дані, які обробляє KPMG

Це дозволяє фізичним особам **перевіряти законність** обробки.

KPMG **повинна своєчасно відповідати на такі запити (DSAR)** , інакше можуть виникнути проблеми з нашими регуляторами.

У випадку отримання вами запиту на доступ **повідомте про це, використовуючи ваші локальні процедури отримання таких запитів,** або, якщо ви не впевнені, зверніться по допомогу до вашого Спеціаліста з питань конфіденційності.

Служба, яка обробляє запити, **розглядає запит**, співпрацює з усіма зацікавленими сторонами, необхідними для реагування на запит, і, за необхідності, передає запит на розгляд вищому керівництву.

Міжнародна передача даних

У глобальній мережі фірм KPMG

- Персональні дані **можуть бути передані** за межі країни, в якій вони були зібрані, включаючи країни за межами ЄЕЗ, для цілей здійснення законної господарської діяльності відповідно до чинного законодавства.
- Відповідно до чинного законодавства, фірми KPMG **можуть зберігати персональні дані** в сховищах, які експлуатуються іншими фірмами KPMG та/або третіми особами від імені фірм KPMG за межами країни, в якій ці дані були зібрані.
- Персональні дані **не повинні передаватися** до іншої країни, якщо особа, яка їх передає, не має впевненості в тому, що стосовно цих персональних даних забезпечено належний рівень захисту, як того вимагає чинне законодавство.
- У випадку кожної фірми KPMG належний рівень захисту забезпечується **Угодою про передачу даних між фірмами**, яка є обов'язковою для дотримання кожною фірмою KPMG.

Третім сторонам за межі мережі KPMG

- Фірми KPMG гарантують, що **у випадках передачі персональних даних третім особам за межі мережі KPMG** для обробки (наприклад, постачальникам послуг KPMG для підтримки бізнесу KPMG), така передача буде здійснюватися лише за умови належного захисту персональних даних.
- Фірми KPMG досягатимуть цього шляхом укладання **письмових угод** із третіми сторонами, які накладають на них зобов'язання, що відображають вимоги цієї політики.

Сумніви чи занепокоєння

Якщо у вас виникнуть сумніви щодо міжнародної передачі даних, повідомте про це партнера по проєкту, а у випадку загальних питань консультуйтеся з вашим **Спеціалістом з питань конфіденційності (PL)**.

Висновок

Висновок

Ви завершили курс і тепер повинні:

- Розуміти ключові загрози для KPMG та її персоналу
- Розуміти, як приймати правильні рішення, дотримуючись політик KPMG щодо захисту інформації та конфіденційності даних
- Знати, як захистити конфіденційну інформацію (включно з інформацією KPMG та клієнта) у всіх місцях, де працюють або можуть обговорювати робочі питання співробітники KPMG
- Розуміти фінансові, юридичні, регуляторні та репутаційні наслідки для бізнесу, клієнтів і персоналу KPMG у разі незахищеності конфіденційної інформації
- Розуміти, що таке персональні дані та чому важливо їх захищати
- Розуміти 10 Принципів конфіденційності даних KPMG і те, як застосовувати їх як розпорядник даних або обробник даних
- Знати ключові кращі практики захисту персональних даних
- Знати різні механізми міжнародної передачі персональних даних
- Розуміти, до кого звертатися, та які подальші кроки робити, коли вам стає відомо про можливе або фактичне порушення інформаційної безпеки або втрату даних

Якщо вам потрібно повідомити про порушення безпеки

Порушення безпеки - це "будь-яка подія, яка може поставити під загрозу конфіденційність, приватний характер, цілісність або доступність нашої інформації чи інформаційних систем". Це не обов'язково має бути подія, про яку ви знаєте, а просто щось, що викликає у вас занепокоєння, що нашій інформації може загрожувати небезпека. Це може бути:

- Втрата будь-якого портативного пристрою (наприклад, ноутбука, мобільного телефону, планшета або накопичувача) або документів
- Витік даних через несанкціонований доступ до мережі
- Загроза шкідливого програмного забезпечення через вибір посилання або вкладення в електронному листі
- Ваші облікові дані для входу могли стати відомі комусь іншому
- Якщо ви помилково надіслали конфіденційний електронний лист не тій людині або перенаправили конфіденційну інформацію іншим способом
- Несанкціоновані відвідувачі в приміщеннях KPMG
- Якщо ви знаєте або підозрюєте, що процедури інформаційної безпеки в проєктах або завданнях не були дотримані належним чином
- Якщо ви підозрюєте, що не уповноважена особа стала свідком обговорення конфіденційної інформації або підслухала розмову
- Використання несанкціонованої електронної пошти або засобів обміну файлами
- Встановлення несанкціонованого або неліцензійного програмного забезпечення (проконсультуйтеся з службою ITS вашої Фірми-члена)

Негайно повідомляйте про фактичні або підозрювані порушення безпеки, щоб можна було швидко вжити відповідних коригувальних заходів. Дотримуйтесь процедури надання інформації, прийнятої у вашій Фірмі-члені, наприклад, зверніться до IT-служби або місцевого підрозділу з управління ризиками.

Якщо інцидент пов'язаний з клієнтом, спочатку зверніться за порадою до місцевого підрозділу управління ризиками. Не проводьте обговорення з клієнтом, поки не буде узгоджена відповідна реакція KPMG.

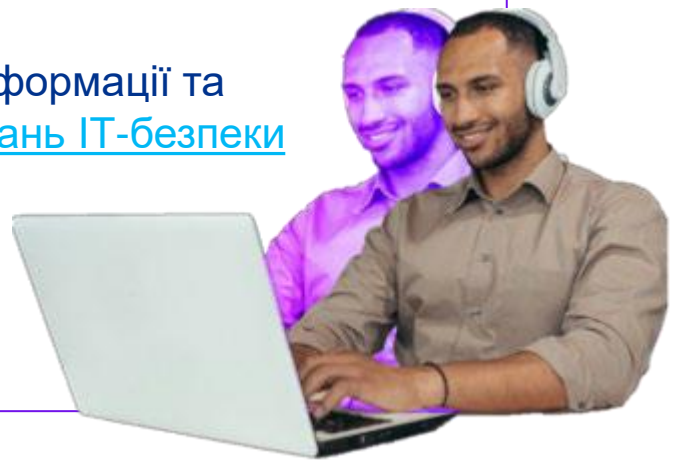
Додаткова інформація та контакти

Загальні запити
Якщо у вас виникнуть запитання щодо **цього курсу чи його змісту**, ви можете звернутися до таких служб Глобальний навчально-інформаційний підрозділ з питань захисту інформації, і Глобальний підрозділ з питань захисту даних.

Відвідати сторінки порталу можна за посиланнями:
Глобальний навчально-інформаційний портал з питань захисту інформації
Глобальний портал з питань захисту даних

Локальні контакти
Якщо у вас виникнуть запитання щодо місцевої Політики з питань захисту інформації та конфіденційності даних, зв'яжіться зі своїм Національним спеціалістом з питань IT-безпеки (NITSO)

- ua-sgua-fmethicsandindependence@kpmg.ua (Відділ контролю якості та управління ризиками)
- ua-fmkieihl@kpmg.ua (Підрозділ з питань захисту даних)



Курс завершено.
Дякуємо

kpmg.ua

Класифікація документа: Публічно