COVID-19. Как безопасно работать из дома

Поскольку COVID-19 вынуждает нас перейти от «Работы в офисе» к «Работе дома», мы должны адаптироваться и сохранять фокус на кибербезопасности во всех ее аспектах.

Безопасное окружение
Постарайтесь выделить комнату в качестве домашнего офиса, заприте дверь, если сможете. Убедитесь, что приватные разговоры остаются конфиденциальными, отключив Alexa и Google Assistant.

Поддержка политики чистого стола
Убедитесь, что все бумажные копии конфиденциальной информации хранятся вне поля зрения и надежно защищены, когда они не используются. По возможности, уничтожайте бумажные носители, если в них больше нет необходимости.

Блокировка экранов
Блокируйте экраны, когда не используете рабочее устройство, и выключайте устройства по окончании рабочего дня. Не оставляйте ноутбуки на виду, когда они не используются.

Установка надежных паролей
Защитите свое рабочее устройство надежными паролями, рассмотрите возможность использования менеджера паролей.

Держать рабочие и личные устройства отдельно
Не используйте рабочие устройства для загрузки личных приложений или инструментов для проведения конференций без согласования. Будьте дисциплинированны в использовании личных устройств для персонального просмотра веб-страниц.

Подключение через VPN
Подключайтесь через VPN, чтобы убедиться, что ваше интернет-соединение зашифровано и ваша информация и онлайн-активность защищена.

Помнить о своей конфиденциальности
Сохраняйте конфиденциальность и будьте в курсе того, что находится в фоновом режиме вашей веб-камеры. Убедитесь, что вы знаете, кто участвует в ваших конференц-звонках.

Безопасные точки доступа Wi-Fi
Убедитесь, что беспроводные маршрутизаторы используют WPA2 и защищены надежными паролями.

Знайте о фишинговых атаках на тему COVID-19

Организованные преступные группы используют нашу озабоченность по поводу COVID-19 в качестве мишени для целого ряда афер.

Обращайте внимание на следующие знаки:

Начало с общего приветствия вроде «Дорогой коллега»

Плохая грамматика или орфографические ошибки

Запрос личных/финансовых данных

Предложение приобрести лекарство, тест на вирус или дефицитные предметы

Просьба о благотворительных пожертвованиях по необычным каналам

Требование срочных действий

Что делать, если вы уже перешли по ссылке?

Самое главное - не паниковать

Откройте ваше антивирусное программное обеспечение и запустите полное сканирование. Внимательно следуйте всем инструкциям.

Свяжитесь с вашим IT-отделом - они расскажут вам, что нужно сделать дальше.

Если вас обманом заставили сообщить свой пароль, вы должны изменить его как можно скорее.

Контакты:

Константин Аушев
Руководитель Группы консультирования в области ИТ и кибербезопасности
Директор
T: +7 727 298 08 98
E: kaushev@kpmg.kz

kpmg.kz