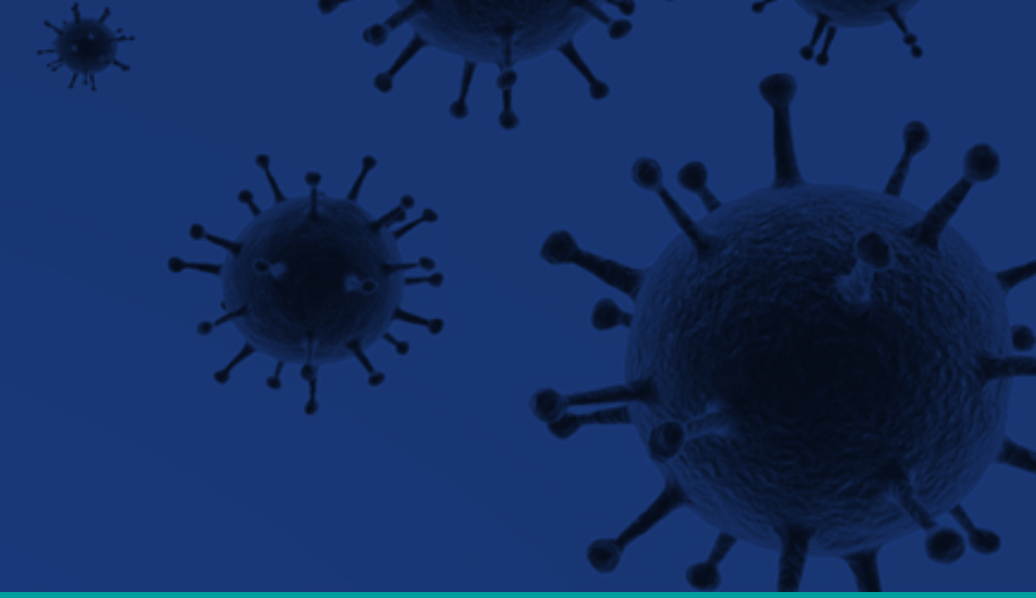


COVID-19: fraudes e golpes Como se proteger?

COVID-19 criou consequências anteriormente inimagináveis para a nossa sociedade. O crime organizado se adaptou rapidamente a esta crise, orquestrando campanhas em larga escala para defraudar clientes bancários, utilizando-se do medo e ansiedade relacionados à COVID-19. Nestes tempos incertos e difíceis, os defraudadores aproveitam-se, de forma oportuna, no medo e na incerteza criados por uma emergência de saúde pública, procurando tirar proveito do desejo do público de recuperar o sentimento de segurança e proteção.

Globalmente, vimos um aumento crescente de golpes associados à COVID-19. *Hackers* de computador e telefone estão tentando ao máximo tirar vantagens dessa pandemia, buscando atrair possíveis vítimas a realizar *downloads* de documentos infectados através de links suspeitos. Os criminosos estão utilizando o crescente número de buscas e a curiosidade sobre o vírus na internet para criar programas maliciosos e escondê-los em arquivos relacionados com o coronavírus.

Além disso, à medida que os governos preparam grandes pacotes de estímulo em resposta à pandemia e começam a fornecer apoio fiscal aos seus cidadãos, o risco de serem defraudados por golpes relacionados com a COVID-19 continuará provavelmente a aumentar.

No mesmo sentido, as medidas de combate à pandemia incrementam riscos relacionados à interação com o setor públicos e a doações governamentáis.

Para alguns segmentos de mercado como os setores de serviços financeiros, telecomunicações, automotivo, industrial *manufacturing*, consumo e varejo e life sciences, além da indústria de farmacêuticos, existem muitos desafios.

Esses setores já começaram a fornecer uma resposta sem precedentes e a trabalhar com seus próprios problemas de continuidade de negócios. A demanda vem superando a oferta, pois os clientes preocupados inundam os *call centers*, uma vez que as tipologias de fraude mudam quase que de hora em hora.

Algumas das potencias fraudes relacionadas com a COVID -19 incluem:

Fraudes tecnológicas

Fraudes comerciais e contratuais

Fraudes em doações e desvio de conduta

Como se proteger?

Compliance focado em gestão de crise

Cyber Secutiry e Forensic Technology

Fraud risk management

Algumas das potenciais fraudes relacionadas com as COVID-19 incluem:

Fraudes tecnológicas

01

Phishing
Os impostores que afirmam ser membros de autoridades sanitárias nacionais e internacionais de renome, como o Centro de Controle e Prevenção de Doenças dos EUA (CDC) ou a Organização Mundial de Saúde (OMS), atraem vítimas com e-mails, anexos, links ou redirecionamentos maliciosos para atualizações acerca da COVID-19, medidas de contenção contra o vírus, mapas de exposição / propagação e novas formas de proteção contra o vírus. Uma vez abertos, esses anexos ou links infectam o dispositivo do computador / telefone com malware ou expõem dados pessoais sensíveis, informações de cartão de crédito etc. Esses dados podem ser transmitidos ao hacker.

02

COVID-19 – sites fraudulentos
Houve um aumento significativo de novas tipologias de risco de fraude, principalmente relacionadas ao registro de um grande número de domínios da internet "COVID". Esses sites parecem endereços de organizações oficiais, mas carregam o malware para infectar os computadores / dispositivos telefônicos.

03

Comprometimento do e-mail corporativo
O aumento do trabalho remoto, acompanhado de atualizações em diversas organizações relacionadas à COVID-19, abriu espaço para fraudadores atingirem empresas e seus funcionários.Usando emails disfarçados de atualizações da COVID-19, os fraudadores tentam induzir os funcionários a entregar suas credenciais solicitando que eles façam login num portal falso de "COVID-19". Depois que o funcionário insere suas credenciais, o fraudador pode ter acesso irrestrito às contas e à rede de negócios da organização.

04

Ataques de ransomware
Instituições governamentais e organizações comerciais estão vendo um aumento nos ataques de ransomware. Nesse tipo de ataque, os servidores ficam compromissados e depois são criptografados. O ataque bloqueia o sistema operacional e os arquivos do usuário-final tornando-os inacessíveis até que algum resgate seja pago (geralmente através de bitcoins) para o hacker. Devido à quarentena imposta pelos governos, o acesso remoto e o trabalho em casa se tornaram uma norma. Esperamos um aumento nos ataques de ransomware com o objetivo de prejudicar os servidores de TI e infraestrutura das empresas para que seja solicitado o resgate.

05

Golpe em aplicativos de celular
Os fraudadores estão desenvolvendo ou manipulando aplicativos para celular que, externamente, parecem rastrear a propagação da COVID-19. No entanto, uma vez instalado, o aplicativo infecta o dispositivo do usuário com malware que pode ser usado para obter informações pessoais, dados confidenciais ou detalhes de contas/cartões bancários.

Algumas das potenciais fraudes relacionadas com as COVID-19 incluem:

Fraudes Comerciais e contratuais

01

Educação Online:
Com o fechamento de escolas e instituições de ensino superior, os pais estão cada vez mais se inscrevendo em vários aplicativos on-line de tecnologia educacional para auto-aprendizado, e os fraudadores também são proativos em suas atividades. Eles se conectam com suas vítimas, fingindo ser um representante de aplicativos educacionais conhecidos e oferecem descontos substanciais para se registrar no link enviado por eles.

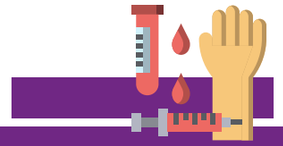
02

Golpes de Suprimentos / Produtos:
Tirando proveito da atual escassez de suprimentos e do desespero público por recursos, os fraudadores estabeleceram lojas on-line falsas que vendem suprimentos médicos atualmente em demanda, como máscaras cirúrgicas e desinfetantes para as mãos. Depois que o pagamento é realizado, os fraudadores ficam com o valor pago e não realizam a entrega do produto comprado. Em igual sentido, a dificuldade de usar a cadeia de fornecedores normal leva empresas a recorrerem a terceiros que podem ter histórico e reputação que acabem por manchar a sua imagem.

03

Medicamentos Falsificados:
Devido à diferença entre a demanda e a oferta de medicamentos essenciais, existe uma grande possibilidade de medicamentos falsificados serem distribuídos e oferecidos para laboratórios / farmácias e possivelmente até no mercado on-line. O público em geral geralmente não consegue identificar facilmente a diferença entre produtos originais e potencialmente falsificados, portanto, as chances de atrair vítimas para tais esquemas são altas.

04



Teste Covid-19 e golpes de tratamento:
O crescente pânico com relação a contração do vírus, criou grupos de pessoas que procuram diversas formas para evitar a contração do vírus, bem como a procura de testes informais para serem realizados sem a anuência do governo (para evitar a ordem de quarentena, para não ficar longe de familiares, etc). Usando mídias sociais e fóruns online, os fraudadores podem promover kits de testes falsos, produtos de tratamento etc., alegando prevenir e curar a doença. Isso inclui a promessa de vacinas, curas falsas e métodos de tratamento não comprovados.

05

Provedores de Assistência Médica:
Fraudadores podem se passar por médicos, enfermeiros, paramédicos, administradores de hospitais, etc., alegando ter tratado, com sucesso, um amigo ou parente conhecido. Dessa forma, atraem vítimas em troca de pagamento pelo referido tratamento contra o vírus.

Algumas das potenciais fraudes relacionadas com as COVID-19 incluem:

Fraudes em doações e desvio de conduta

01

Golpes de doação
Em tempos de crise,não é incomum sentir-se responsável por ajudar a reduzir o impacto na comunidade e auxiliar os menos afortunados. Os fraudadores atacam esse desejo, solicitando doações para instituições de caridade inexistentes. Em igual sentido, doações representam sempre um risco de conformidade se não realizadas com as cautelas devidas: aquelas feitas a instituições públicas expõem a empresa a alegações de corrupção e as feitas a entidades privadas precisam ser adequadamente verificadas de modo a previnir futuras alegações de fraude.

02

Desvios de conduta
A alteração nas rotinas normais das empresas abre espaço para diversas fraudes internas que podem ter a empresa como vítima (como desvios financeiros, pagamentos em duplicidade etc.) ou mesmo fraudes que busquem artificialmente inflar seus resultados (como fraudes contábeis). Em igual sentido, a pressão por resultados em uma situação de adversidade aumenta o risco de práticas ilícitas que podem trazer graves prejuízos legais e reputacionais, como infrações concorrenciais, de corrupção etc.

Como se Proteger?

Compliance focado em gestão de crise

Existem várias maneiras de ajudar a proteger você, seus entes queridos e sua empresa de serem vítimas de golpes da COVID-19.
A importância de reduzir a vulnerabilidade é garantir que as pessoas continuem cientes de como os criminosos estão tentando tirar proveito da crise da saúde global e de que responder aos desafios não necessariamente significa expor organizações a riscos de longo prazo.

01

Verifique os antecedentes antes de doar para instituições de caridade ou campanhas de financiamento coletivo. Desconfie de qualquer negócio, instituição de caridade ou indivíduo que solicite doações em dinheiro, pelo correio, via transferência de fundos ou outros canais incomuns e realize um Integrity Due Diligence antes qualquer doação.

02

Tenha um procedimento de gestão de crises organizado e estabeleça um programa de Compliance Analytics para garantir que seus controles internos e suas rotinas de prevenção, detecção e resposta a quebras de integridade estejam adequadamente adaptadas às novas práticas e procedimentos do negócio e ao seu plano de resposta.

03

Adapte suas rotinas de compliance ao novo cenário de riscos e garanta que as interações com órgãos governamentais e concorrentes estejam adequadamente registradas e controladas.

04

Não confunda agilidade com ausência de controle. Garanta que prestadores de serviço e fornecedores contratados passem por um procedimento de diligência básico e que seus contratos incluam cláusulas anticorrupção claras.

05

Navegue com organização pelo mar regulatório. As diversas modificações legais e regulamentares editadas pelas autoridades no combate à crise representam oportunidades, mas também aumentam o risco de más interpretações e quebras de conformidade. Mapeie as alterações com cuidado e implemente um sistema de revisão de procedimentos e decisões.

Como se Proteger?

Cyber Security e Forensic Technology

01

Proteja e controle o acesso remoto e a infraestrutura de TI, e restrinja o acesso aos IDs de usuário (interno / externo). Revogue todas as conexões diretas nos servidores de fora do escritório. Monitore o desempenho do servidor e da rede e defina alertas.

02

Limite e registre o uso de aplicativos que fornecem acesso remoto, reforçe as redefinições obrigatórias de senhas e crie autenticação de dois fatores em ativos críticos de TI.

03

Verifique se os software *anti-malware*, *anti-ransomwar*e e antivírus estão instalados nos dispositivos e se estão atualizados. Garanta que as correções do sistema operacional estejam sempre atualizadas. Evite a instalação de *freeware* nos sistemas de TI, pois eles podem conter *malware* ou "cavalos de troia" ocultos

04

Conecte-se à internet usando pontos de acesso de Wi-Fi que são seguros e conexões de banda larga. É altamente recomendável conectar-se à internet usando uma rede privada virtual.

05

Evite usar sites públicos de compartilhamento de arquivos, a menos que autorizado pela política da sua organização.

Como se Proteger?

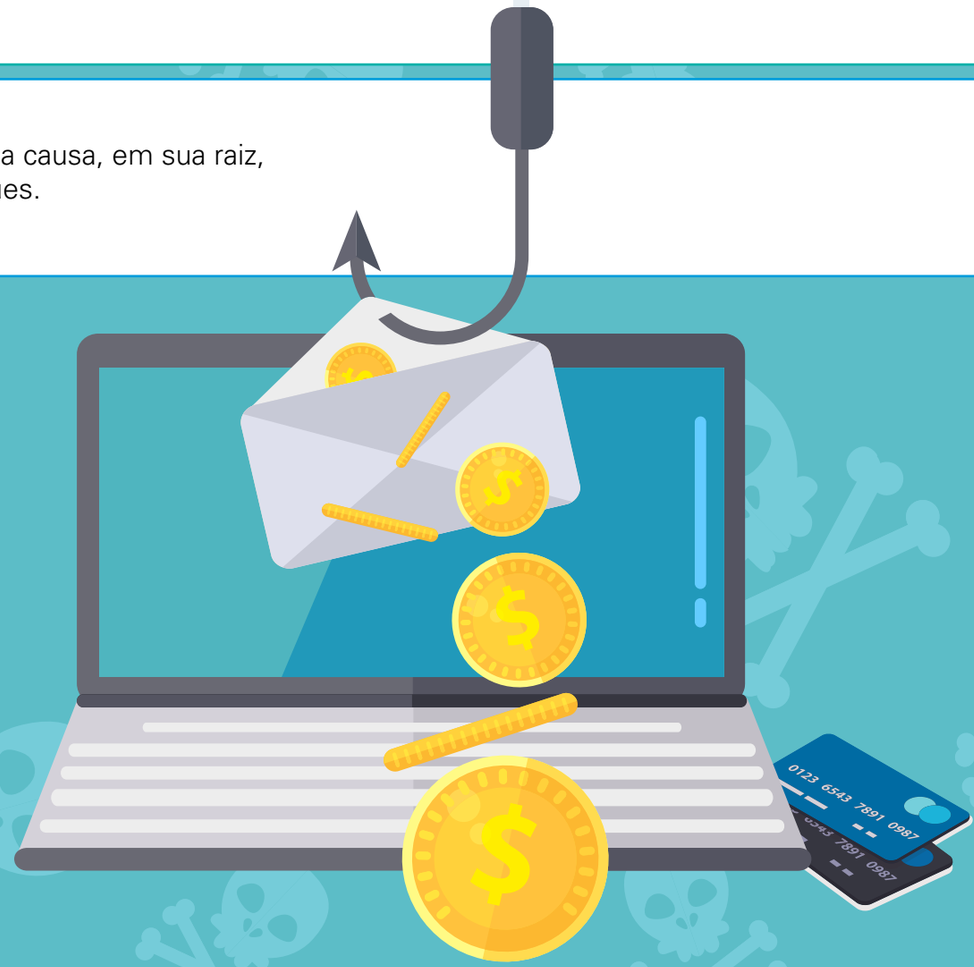
Fraud risk management

01

Não descarte violações ou incidentes, pois podem indicar um problema maior

02

No caso de um ataque cibernético investigue a causa, em sua raiz, para se proteger e se prevenir de novos ataques.



Fale com o nosso time

Emerson Melo
Sócio-líder de Forensic da KPMG no Brasil
Tel.: (11) 3940-4526
emersonmelo@kpmg.com.br

Diogo Dias
Sócio-líder de Risk Advisory Solutions da KPMG no Brasil
Tel.: (11)3940-3177
dsdias@kpmg.com.br

Rafael Weksler
Sócio-líder de Risk Advisory Solutions da KPMG no Rio de Janeiro
Tel.: (21) 2207-9232
rweksler@kpmg.com.br

Alexandre Massao
Sócio de Forensic & Litigation da KPMG no Brasil
Tel.: (11) 3940-6379
amhabe@kpmg.com.br

Marcelo Gomes
Sócio de Forensic & Litigation da KPMG no Brasil
Tel.: (11) 3940-4829
marceloagomes@kpmg.com.br

Raphael Soré
Sócio de Forensic & Litigation da KPMG no Brasil
Tel.: (11) 3940-5958
rsore@kpmg.com.br

Patrícia Silva (MG)
Sócia-diretora de Risk Advisory Solutions da KPMG no Brasil
Tel.: (31) 2128-5740
pssilva@kpmg.com.br

Ser criativo
transforma negócios.

#KPMGTransforma

Baixe o nosso APP

kpmg.com.br /kpmgbrasil