FRAUDES DIGITAIS

campos thomaz
& meirelles advogados

ÍNDICE:

1 INTRODUÇÃO

— O que é Fraude Digital?

A fraude é um ato ardiloso, enganoso e de má-fé que tem por objetivo lesar ou ludibriar alguém para trazer algum tipo de vantagem, geralmente financeira, ao fraudador sobre a vítima. A fraude abrange um universo complexo, de diferentes naturezas de crimes e penas previstas no Código Penal Brasileiro, e pode causar danos irreparáveis à vítima, sejam eles financeiros, psicológicos ou de imagem.

A fraude digital, por sua vez, pode se caracterizar como qualquer situação em que dados são utilizados indevidamente para cometer crimes cibernéticos, gerando prejuízos às vítimas (que podem ser consumidores ou empresas).

No caso de empresas, fraudes digitais podem se tornar incidentes de dados pessoais, causando consequências ainda mais graves.

— Cenário Atual

Nos últimos anos, o aumento do número de usuários utilizando os meios digitais resultou em uma rápida adaptação dos negócios brasileiros em digitalizar suas operações. Este contexto favorece a expansão de crimes, em razão da maior facilidade em roubar dados e maior dificuldade em identificar criminosos em comparação ao meio físico.

A pandemia da Covid-19, por sua vez, acelerou ainda mais esse processo. Com o isolamento social, a internet passou a ser utilizada cada vez mais para diferentes objetivos, como o trabalho (home office) e realização de transações digitais.

Com isso, o ambiente digital passou a ser cada vez mais visto como uma oportunidade de aplicação de fraudes.

— Dados de 2021

Brasil é o 3º país do mundo mais afetado por fraudes

57% das empresas no Brasil são afetadas por fraudes digitais*

Setores mais afetados: instituições financeiras, marketplaces e e-commerces

R$ 5,8 bilhões em prejuízo por fraudes em sites de comércio eletrônico, vendas diretas, serviços financeiros e de telecomunicações**

Apenas 39% das organizações consideram a segurança digital como prioridade***

* Pesquisa publicada pelo Instituto Datafolha em parceria com o MasterCard (https://www.mastercard.com/news/latin-america/pt-br/noticias/comunicados-de-imprensa/pr-pt/2021/junho/57-das-empresas-brasileiras-sao-alvos-de-fraudes-e-ataques-digitais-com-alta-ou-media-frequencia-revela-estudo-da-mastercard/#:~:text=Sobre%20o%20Bar%C3%B4metro%20da%20Seguran%C3%A7a,25%20de%20fevereiro%20de%202021.)

**Pesquisa publicada pelo ClearSale (https://blogbr.clear.sale/mapa-da-fraude-2021-clearsale)

***Pesquisa publicada pelo Instituto Datafolha em parceria com o MasterCard (https://www.mastercard.com/news/latin-america/pt-br/noticias/comunicados-de-imprensa/pr-pt/2021/junho/57-das-empresas-brasileiras-sao-alvos-de-fraudes-e-ataques-digitais-com-alta-ou-media-frequencia-revela-estudo-da-mastercard/#:~:text=Sobre%20o%20Bar%C3%B4metro%20da%20Seguran%C3%A7a,25%20de%20fevereiro%20de%202021.)

— Lei 14.155/2021 – Novas punições para fraudes e golpes digitais no Brasil

A Lei 14.155/2021 veio como uma resposta ao cenário de aumento de fraudes digitais cometidas no país ao longo dos últimos anos. Com a nova lei, crimes cibernéticos como fraude, furto e estelionato praticados com o uso de equipamentos eletrônicos (como celulares, computadores e tablets) passaram a ser punidos com penas maiores. As principais alterações promovidas pela lei incluem:

- Se o crime for cometido contra um idoso ou vulnerável, a pena pode ser majorada de um terço ao dobro
- Aumento da pena para circunstâncias em que a invasão resultar na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas ou no controle remoto não autorizado do dispositivo invadido (de seis meses a dois anos mais multa, para dois a cinco anos e multa)
- As penas previstas podem aumentar de um terço a dois terços se o crime for praticado por meio de servidor mantido fora do território nacional
- Aumento da pena para a invasão de dispositivos eletrônicos alheios (a detenção prevista passou de três meses a um ano mais multa, para um a quatro anos)

2 PRINCIPAIS GOLPES E RISCOS

Phishing

O phishing é considerado um dos golpes digitais mais comuns. Ele se caracteriza pela tentativa de adquirir ilicitamente dados de terceiros, como senhas, dados financeiros, bancários ou números de cartões de crédito. Para isso, costuma-se enviar um link falso de uma instituição bancária ou uma promoção falsa, e o usuário, acreditando tratar-se de página verdadeira, compartilha seus dados.

Malware

O termo malware é usado para classificar todo tipo de software malicioso (e.g., worms, spyware, cavalo de troia, ransomware) usado para causar algum prejuízo ao dispositivo invadido. O malware pode ser utilizado para controlar o computador ou para um ataque direto, no qual o código malicioso consegue capturar dados da vítima. O malware pode se propagar de diversas formas, como através de e-mails maliciosos na forma de campanhas de spam ou envio de arquivos falsos que infectam o dispositivo quando abertos.

Ransomware

Ransomware é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia. Além de infectar o equipamento, o ransomware também costuma buscar outros dispositivos conectados, locais ou em rede, e criptografá-los. É comum que se exija o pagamento de resgate (ransom) para restabelecer o acesso ao usuário, normalmente por bitcoins. O ransomware pode se propagar de diversas formas, embora as mais comuns sejam através de e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link, ou explorando vulnerabilidades em sistemas desatualizados.

Shadow IT e roubo de equipamentos

"Shadow IT" é o termo dado às práticas não oficiais, não autorizadas e desconhecidas pela gestão de TI de uma empresa, como o uso de softwares não autorizados. Essas condutas, por não serem monitoradas, podem representar ameaças de segurança para os dados corporativos. De modo semelhante, o roubo de equipamentos corporativos ou pessoais que contenham dados de trabalho (como no caso do "Bring Your Own Device") pode apresentar riscos graves à segurança da empresa.

Invasão por Brechas de Segurança

As brechas de segurança são uma porta aberta para fraudes digitais. Essa brecha pode ocorrer por diversos motivos, como uma falha de segurança no servidor, a ausência de uma atualização necessária do sistema ou até a falta de controle de acesso à sala de servidores.

Boletos bancários falsos

Essa fraude é caracterizada pelo envio de um boleto falso em nome de alguma empresa ou instituição para o e-mail da vítima, que acredita se tratar de um boleto verdadeiro (e.g., um boleto para o pagamento da conta de luz ou de telefone). Ao realizar o pagamento, a vítima faz o depósito na conta dos criminosos.

Fraudes de Identidade por e-mail e WhatsApp

O envio de links maliciosos por e-mail ou WhatsApp se tornou cada vez mais comum. Criminosos enviam links com assuntos de interesse público para atrair vítimas que, ao clicar no link falso e inserir os dados para um cadastro, têm seus dados pessoais roubados (e.g., cadastro para auxílio emergencial durante a pandemia do Covid-19). Outros golpes envolvem especificamente o WhatsApp, como a clonagem de contas do aplicativo de mensagens. Neste tipo de fraude, o criminoso se passa por uma empresa e solicita o envio do código de verificação do WhatsApp, que é enviado por SMS para o celular da vítima, para validar uma falsa solicitação da suposta empresa. Em posse do código, o criminoso consegue clonar o WhatsApp da vítima e passa a ter acesso à sua lista de contatos e grupos, podendo, por exemplo, pedir dinheiro para amigos e familiares da vítima. .

Fraude do Pix

Com a popularização do Pix, que revolucionou as movimentações bancárias ao viabilizar a realização de transferências ou pagamentos em poucos segundos e sem cobrança de taxas, vieram também os golpes relacionados a essa nova ferramenta. Enquanto alguns são apenas uma adaptação de velhos golpes, outros exploram as características próprias do novo sistema de pagamento. Um dos golpes aplicados, e já responsável pelo furto de milhões de reais, é o da "falha do Pix". Este golpe promete ao usuário a devolução em dobro do dinheiro transferido a determinadas contas via Pix com a justificativa de existir uma falha de segurança de determinada instituição financeira. Muitos usuários tendem a realizar uma transferência de forma impulsiva e, depois de refletir melhor sobre a fraude, já é tarde demais para reaver o dinheiro.

Fraudes Digitais

Com o intuito de aumentar a segurança do Pix, o Banco Central vem divulgando novas ferramentas para evitar fraudes e auxiliar possíveis vítimas, como o Mecanismo Especial de Devolução (MED) e o Bloqueio Cautelar. Com o Bloqueio Cautelar, se o banco onde o golpista recebe os recursos desconfiar de uma operação, ele pode avaliar a existência de indícios de fraude e bloquear os recursos por até 72 horas. Já o Mecanismo Especial de Devolução pode ser acionado tanto pela instituição bancária como pela vítima do suposto golpe. Para tanto, é necessário registrar um boletim de ocorrência e comunicar o ocorrido à sua instituição financeira pelos canais oficiais de atendimento ao cliente. Se o golpe for constatado, o dinheiro volta para a conta da vítima.

3 MEDIDAS INTERNAS DE SEGURANÇA

Para se prevenir de fraudes digitais, é necessário planejamento, elaboração de estratégias e treinamentos internos para capacitar todos os colaboradores de uma empresa.

Reconhecer sua vulnerabilidade aos ataques: Atualmente, qualquer organização, independente do porte, está sujeita a fraudes digitais. Portanto, reconhecer a vulnerabilidade de sua organização e dar importância para esse risco é o primeiro passo. A partir disso, será possível identificar as vulnerabilidades e criar estratégias para a adequação e treinamento da empresa.

Elaborar uma política de segurança: A elaboração de uma política de segurança da informação é essencial para proteger qualquer organização contra fraudes digitais. Dentre os aspectos a serem abordados na política de segurança, pode-se destacar a criação de senhas fortes que sejam alteradas com frequência, regras gerais para armazenamento de documentos, realização de downloads e anexos, e o que fazer em caso de incidente.

Elaborar uma política de segurança: A elaboração de uma política de segurança da informação é essencial para proteger qualquer organização contra fraudes digitais. Dentre os aspectos a serem abordados na política de segurança, pode-se destacar a criação de senhas fortes que sejam alteradas com frequência, regras gerais para armazenamento de documentos, realização de downloads e anexos, e o que fazer em caso de incidente.

Treinamento de funcionários: Além da implementação da política de segurança, é preciso promover treinamentos periódicos aos colaboradores da organização, para que eles compreendam as regras de forma clara e estejam capacitados a reconhecer os golpes e saber o que fazer caso ocorra.

— Dicas Práticas de Como Evitar Fraudes Digitais

- Verifique se a página utiliza conexão segura. Sites de e-commerce ou Internet Banking confiáveis utilizam conexões seguras quando dados relevantes são solicitados
- Utilize mecanismos de segurança, como programas antimalware, firewall e filtros antiphishing

- Realize sempre as atualizações de segurança disponíveis em seu computador, de modo a evitar vulnerabilidades no sistema
- Cuidado com e-mails com anexos suspeitos, que possam conter códigos maliciosos ou que induzam o usuário a seguir um link suspeito
- Fique atento a e-mails recebidos que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em links
- Verifique sempre os links enviados a você. Golpistas costumam usar técnicas para ofuscar o link real para o phishing, mas ao posicionar o mouse sobre o link, muitas vezes é possível ver o endereço real da página falsa ou código malicioso
- Não responda a e-mails de spam
- Nunca anote senhas e outras informações confidenciais em lugares visíveis ou de fácil acesso (incluindo arquivos não criptografados dentro do seu computador ou pendrive)
- Não use computadores públicos, de terceiros ou computadores que não tenham sistemas de proteção adequados para acessar sua conta, dados sigilosos e arquivos de trabalho
- Evite navegar em sites arriscados e nunca baixe arquivos de sites que não conheça ou que não sejam totalmente confiáveis
- Configure seu navegador de internet para que peça sempre autorização e confirmação antes de baixar ou executar qualquer arquivo ou programa na internet

4 COMO MELHORAR A SEGURANÇA DO SEU CLIENTE?

É extremamente relevante a adoção de medidas para evitar brechas de segurança e, consequentemente, proteger uma empresa e os seus usuários de fraudes e ataques cibernéticos. Veja a seguir algumas das ações que podem ser adotadas:

Mantenha o antivírus atualizado: Mantenha sempre um antivírus eficaz e com as devidas atualizações nos seus equipamentos.

Criptografia de dados: É recomendado que os dados sejam criptografados, dificultando o acesso de terceiros em caso de incidente.

Atualização dos sistemas: Sempre utilize softwares atualizados, para evitar a vulnerabilidade dos seus sistemas e equipamentos.

Exija a criação de senhas fortes: É essencial elaborar senhas fortes para a administração de servidores e sites. Outra prática para a preservação de informações é a solicitação de senhas com letras e números para os usuários ingressarem em determinadas áreas da página.

Background Check: Existem procedimentos disponíveis (como o background check) para a análise de informações fornecidas por clientes, parceiros e fornecedores, a fim de verificar se as informações fornecidas são verdadeiras e confiáveis e evitar fraudes.

Reconhecimento facial: Em alguns serviços, a tecnologia de reconhecimento facial pode auxiliar na redução dos riscos de fraudes de identidade de clientes. Este método de autenticação utiliza técnicas de biometria facial para analisar o rosto do usuário e traçar padrões da face e suas características únicas. Dessa forma, é possível garantir que a pessoa que está tentando acessar a sua plataforma ou realizar uma transação financeira é realmente quem diz ser.

5 O QUE FAZER EM CASO DE FRAUDE?

— Medidas a serem adotadas em caso de fraude

Mesmo com a adoção de medidas preventivas para reduzir o risco de ataques, em algum momento você ou sua organização podem se deparar com alguma fraude digital.

Para isso, é muito importante ter um plano de resposta a incidentes para orientar o gerenciamento de qualquer fraude ou suspeita de incidente de forma célere e apropriada.

— O que fazer em caso de fraude envolvendo dados pessoais?

Caso a fraude envolva o acesso não autorizado, acidental ou ilícito de dados pessoais e possa ocasionar risco para os direitos e liberdades do titular dos dados pessoais, a fraude pode resultar em um incidente de segurança, nos termos da Lei Geral de Proteção de Dados (“LGPD”).

— No caso de incidente de segurança envolvendo dados pessoais, deve-se:

- Acionar o plano de resposta a incidentes da empresa
- Avaliar internamente o incidente, ou seja, sua natureza, categoria e quantidade de titulares de dados afetados, categoria e quantidade dos dados afetados, consequências concretas e prováveis
- Comunicar ao encarregado de proteção de dados (DPO) da organização
- Comunicar ao controlador dos dados (caso você seja o operador), nos termos da LGPD
- Elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas
- Comunicar à Autoridade Nacional de Proteção de Dados (“ANPD”) e ao titular de dados, em caso de risco ou dano relevante aos titulares

Nossos reconhecimentos

Análise Advocacia (2021)

Chambers & Partners Brazil (2021 e 2022)

Leaders League (2021 e 2022)

Transactional Track Record (2021 e 2022)

The Legal 500 (2022)

Conheça nossos
Sócios

Alan Campos Thomaz

Sócio

Tecnologia e Negócios Digitais, Privacidade e Proteção de Dados, Fintechs e Propriedade Intelectual

at@camposthomaz.com

+55 11 9 8375.2627 +1 (650) 6436652

Sérgio Meirelles

Sócio

Societário, M&A, Venture Capital e Wealth

sergio@camposthomaz.com

+55 11 9 7551.9865

Filipe Starzynski

Sócio

Contencioso & Law Enforcement, Consultivo Cível, Imobiliário, Trabalhista e Família

filipe@camposthomaz.com

+55 11 9 7151.9639

Juliana Sene Ikeda

Sócia

Propriedade Intelectual, Tecnologia, Contratos e Life Sciences

juliana@camposthomaz.com

+55 11 9 8644.1613

Nos acompanhe em nossas redes

Assine nossa newsletter