ENGENHARIA SOCIAL

Saiba como evitar possíveis
armadilhas e se proteger de **golpes.** ↘

FEBRABAN
Federação Brasileira de Bancos

1 O QUE É ENGENHARIA SOCIAL?

Os métodos e técnicas usados por golpistas para manipular pessoas para que revelem dados pessoais, corporativos ou comprometam sistemas computacionais são chamados de engenharia social.

A forma de atuação vai desde pesquisas nas redes sociais para obter informações até o uso de malwares – softwares maliciosos.

Dados pessoais e corporativos são ativos valiosos não só para empresas, mas para toda a sociedade.

A cada inovação tecnológica, novas brechas de segurança também são criadas. E os hackers e golpistas se aproveitam dessas falhas usando a engenharia social para cometer crimes, causando prejuízo às vítimas e às empresas.

Aquele que usa a influência e persuasão, com técnicas psicológicas de convencimento ou por meio da tecnologia para enganar e manipular pessoas a revelarem ou concederem acesso a dados pessoais e informações sigilosas, que serão usados na aplicação de golpes visando benefício financeiro ou fraudes contra terceiros, é chamado de engenheiro social.

MALWARE

Termo do inglês, malicious software (software nocivo ou malicioso). É um programa utilizado para infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar danos, alterações ou subtrair informações confidenciais ou pessoais.

Empresas investem muito dinheiro em aspectos técnicos para aumentar a segurança de seus dados e de seus clientes. Criam firewalls, antimalwares e criptografia. Mas ignoram o fator mais vulnerável em um sistema de segurança: **o comportamento humano.**

Se informar e ficar atento ao modo de execução dos golpistas — ou engenheiros sociais — é o jeito mais eficaz de impedir um golpe.

2 ABORDAGEM DO ENGENHEIRO SOCIAL

O engenheiro social coloca em prática o golpe com base em certos descuidos e, muitas vezes, a partir da ingenuidade da vítima, seja pela exposição excessiva de hábitos pessoais em redes sociais, seja pela divulgação a terceiros de senhas, tokens ou quaisquer outras informações sigilosas.

A prática de engenharia social no ambiente empresarial também é comum. Todo ambiente de trabalho dispõe de dados confidenciais e sensíveis, que, em muitas situações, não estão devidamente protegidos.

Documentos esquecidos em impressoras ou copiadoras; papéis reutilizáveis de relatórios e atas de reuniões, contendo assinaturas, números de telefone, e-mails, endereços, agendas, demonstrativos financeiros; crachás expostos fora do ambiente da empresa; catracas sem controle de acesso, muitas vezes são suficientes para "quebrar" todo o sistema de segurança de uma empresa.

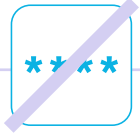
Você deve ter observado que, nos casos mencionados, não foram incluídos meios tecnológicos, os quais também são empregados para aprimorar o processo de ludibriar vítimas, sejam elas pessoas físicas ou jurídicas.

É necessário ficar atento a abordagens em telefonemas. Muitas vezes, as ligações são feitas por indivíduos que se apresentam como conhecidos ou que simulam o contato em nome de instituições reconhecidas no mercado, como seu banco de confiança ou a rede de supermercados que você faz compras habitualmente. Solicitam dados, como senha, login, token, número do CPF, filiação ou outras informações. Em outros tipos de abordagem, pedem endereço de e-mail para envio de anexos, que podem simplesmente, sem que você perceba, abrir a porta para o engenheiro social acessar seu computador ou seu celular.

Tenha cuidado com a exposição excessiva nas redes sociais.

É importante manter-se alerta constantemente, em especial às mensagens de origem duvidosa com arquivos anexados ou indicação de links para você clicar.

As redes sociais são meios de fácil acesso para obtenção de informação por fraudadores e engenheiros sociais. A excessiva exposição da vida pessoal contribui para que o engenheiro social tenha sucesso na aplicação do golpe. Geralmente, esquecemos que estamos revelando hábitos pessoais, preferências, notícias dos familiares, lugares que costumamos frequentar, informações de trabalho, bens etc.




3 IDENTIFICAÇÃO DAS VÍTIMAS E MÉTODOS DE EXECUÇÃO DA ENGENHARIA SOCIAL

São inúmeras as motivações do engenheiro social para aplicação do golpe: espionagem industrial para obtenção de informações sensíveis, antecipadas e valiosas; fraudes contra terceiros; busca por vulnerabilidades nos sistemas de proteção; ou "simples brincadeira".

Todos podemos ser vítimas se não estivermos atentos e preparados. Somos suscetíveis a fornecer dados relevantes, sejam relacionados a uma pessoa ou a uma empresa. Qualquer pessoa, independentemente de cargo ou classe social, pode representar um alvo, uma vítima potencial para o engenheiro social. Por isso, fique atento!

A engenharia social possui três principais vetores de ataque. Conheça, a seguir, os métodos mais utilizados para a prática de golpes.

Sites Falsos

Uma forma altamente eficaz de execução da engenharia social é a criação de sites fraudulentos, apresentados às vítimas basicamente em dois formatos:

1. Imitação de sites de grandes instituições, que visam induzir a vítima a acreditar que são confiáveis e legítimos;

Exemplo:

mercadolivre.com.br x rnercadolivre.com.br

Golpistas também usam fontes específicas para confundir o usuário ao clicar em um link. No caso acima, a letra “r” e a letra “n” parecem um “m”.

2. Sites com conteúdo atrativo para que a vítima seja persuadida a informar dados pessoais para fins cadastrais ou mediante oferecimento de descontos e cupons.

E-mails (SPAM)

Método que consiste no envio de e-mails, que, aparentemente, são originados de fontes confiáveis. Esses e-mails têm como objetivo obter dados pessoais ou informações sensíveis mediante apresentação de conteúdo atrativo que desperte na vítima o interesse em clicar em um link que a direciona ao site falso. Esse tipo de e-mail também pode conter arquivos maliciosos que infectam celulares, tablets ou computadores.

Veja alguns exemplos de títulos mais comuns utilizados para prática de engenharia social:

“Intimação da Receita Federal – Você caiu na malha fina”
“Sorteio Dia das Mães – Você ganhou um carro 0 km”
“Resgate seu FGTS já – Clique no link e receba agora”
“Empréstimo facilitado e com a menor taxa de mercado – Contrate agora”
“Ganhe dinheiro fácil”

Redes Sociais
(Facebook, Instagram, LinkedIn, Twitter, TikTok, YouTube)

Com o aumento significativo do número de usuários de redes sociais, golpistas encontraram uma maneira fácil e eficaz de obter informações diversas sobre possíveis vítimas.

Com uma simples pesquisa nas redes sociais, é possível traçar os perfis pessoal, profissional e comportamental das vítimas. As publicações que não possuem controle de exibição a terceiros ficam disponíveis para visualização por qualquer usuário e podem ser uma ferramenta muito útil para aplicação de golpes, pois o engenheiro social já conhecerá um pouco sobre você.

Aplicativos de comunicação Instantânea
(WhatsApp, Viber, Skype, Facebook Messenger, Telegram, Instagram)

São responsáveis por possibilitar o fluxo imediato de imenso volume de informações, tais como fotos, vídeos, notícias, documentos e links. A disseminação de links e de arquivos maliciosos por meio de aplicativos de comunicação instantânea é uma técnica muito eficaz utilizada por golpistas. Por isso, fique atento se os conteúdos e links que você recebe são de contatos conhecidos e de confiança, pois essas ferramentas podem ser utilizadas pelo engenheiro social para abordagem e aplicação de golpes.

Telefone e SMS

A forma mais recorrente da abordagem por telefone é a identificação do golpista como representante de falsa central de atendimento de empresas de telefonia ou de instituições conhecidas, como bancos, administradoras de cartão de crédito ou autoridades de órgãos governamentais.

O engenheiro social é sempre muito educado, cordial e simpático no momento da abordagem. No contato telefônico, por exemplo, ele utiliza técnicas de persuasão e convencimento para induzir a vítima a confirmar dados pessoais, senhas, tokens, número de cartões ou informações corporativas sensíveis. Esse método é popularmente conhecido como vishing (voice + phishing) e consiste na prática criminosa por meio da rede de telefonia com o objetivo de obter vantagens ilícitas, como realizar compras pela internet com os dados dos cartões das vítimas, fazer saques em dinheiro ou solicitar depósito de determinado valor para liberação de falsos empréstimos, concedidos por instituições de fachada.

Outra técnica utilizada pelos engenheiros sociais para enganar possíveis vítimas é o envio de mensagens de texto (SMS), com o intuito de induzir a vítima a baixar malwares em seu dispositivo móvel ou de direcioná-la para um site falso. As mensagens smishing (phishing por SMS) geralmente são criadas para desencadear uma ação imediata, exigindo que as vítimas informem dados pessoais ou confidenciais. Esse método é recorrente em mensagens enganosas, que contêm conteúdos como os exemplificados a seguir:

.

Negativação de CPF, verifique com urgência

Confirme seus dados para evitar o bloqueio de seu cartão de crédito

Você foi sorteado na Promoção do Baú, acesse o link e receba agora

Também podem estar presentes em mensagens que oferecem serviços e produtos não solicitados.

Presencialmente

Engenheiros sociais se aproveitam do descuido e da ingenuidade dos clientes no ambiente de agências bancárias para realizar troca de cartões em terminais de autoatendimento ou para obter informações relacionadas a contas e senhas, agindo como pessoas bem-intencionadas e interessadas em ajudar o próximo.

A verbalização de informações a terceiros em ambientes diversos também apresenta fator de risco. Os engenheiros sociais utilizam dados pessoais divulgados em locais públicos, como restaurantes, aeroportos, elevadores, táxis, hotéis, bancos etc.

É necessário saber como os engenheiros sociais atingem as vítimas, explorando os seguintes sentimentos humanos:

Curiosidade

Abordam assuntos populares ou atrativos para induzir o clique em arquivos maliciosos ou links que direcionam a sites falsos.

Preguiça

Tiram proveito da negligência de alguns funcionários em seguir regras corporativas.

Vaidade

Ofertam falsos produtos e serviços em condições imperdíveis, com o intuito de estimular a futilidade e o poder.

Solidariedade

Criam falsas campanhas de doações, oferecem descontos e promoções; são extremamente prestativos em ajudar em transações nos terminais bancários de autoatendimento.

Ingenuidade

Exploram o desconhecimento técnico e informacional das vítimas.

Confiança

Utilizam o nome de grandes corporações e de entidades governamentais para obter informações.

Ganância

Oferecem falsas oportunidades de ganhos altos em pouco tempo.

Medo

Usam a persuasão e o convencimento para obter informações.

Definitivamente, não existem sistemas de segurança que sejam imunes ao excesso de generosidade ou à ingenuidade do ser humano. Uma pergunta inofensiva, um descuido, uma amizade repentina, a revelação de um segredo importante e é assim que dados pessoais e informações corporativas sigilosas vazam, sistemas são invadidos e empresas podem sofrer grandes prejuízos.

Valendo-se de algumas informações, com paciência, criatividade, apelo sentimental e sob o pretexto de situações de emergência ou até mesmo, para garantir a máxima segurança, escolhendo as pessoas certas, as chances de sucesso do golpe só aumentam.

Por isso, é muito importante estarmos sempre em alerta e em contínua conscientização.

4 COMO SE PROTEGER DA ENGENHARIA SOCIAL?

Dicas úteis para proteger informações pessoais

Proteção no Whatsapp

• Inclua uma senha adicional habilitando a confirmação em 2 etapas.
NUNCA informe o código a ninguém!
Vá em **Configurações > Conta > Confirmação em duas etapas > Ativar**

• Permita que apenas seus contatos tenham acesso à sua foto do perfil.
Vá em **Configurações > Conta > Privacidade > Foto do perfil > Meus contatos**

• Defina quem pode te adicionar a grupos de conversas.
Vá em **Configurações > Conta > Privacidade > Grupos > Meus contatos**

• Você também pode definir o desbloqueio de tela do WhatsApp somente com sua biometria.
Configurações > Conta > Privacidade > Bloqueio de Tela ou Bloqueio por impressão digital

• Não forneça dados pessoais, senhas e informações sensíveis por telefone, e-mail, redes sociais e aplicativos de comunicação instantânea.

• Fique atento: os bancos não solicitam confirmação de dados pessoais relacionados a contas bancárias, senhas e cartões por telefone, SMS, e-mail ou por outros meios. Jamais forneça dados para alguém que se identificar como operador de central de atendimento. Sempre entre em contato com o gerente da sua conta para questionar sobre esse tipo de solicitação.

• Faça controle periódico da fatura de seu cartão de crédito e de seu extrato bancário.

• Se o aplicativo do seu cartão de crédito permite bloquear e desbloquear o seu cartão a qualquer momento, é uma boa ideia liberá-lo apenas ao realizar uma compra.

• Em caso de dúvidas em operações nos caixas eletrônicos de autoatendimento, somente aceite ajuda de funcionário devidamente uniformizado e identificado por crachá do banco.

• Não responda, por quaisquer meios, mensagens de empresas ou instituições desconhecidas.

• Caso receba alguma ligação suspeita, não passe nenhum de seus dados. Termine a chamada, aguarde 5 minutos e entre em contato com a central de atendimento do seu banco pelos canais oficiais - aqueles que você encontra no site da instituição. O tempo de espera é importante para que a sua chamada não seja interceptada pelos fraudadores.

• Fique atento a downloads de arquivos, jogos e aplicativos em dispositivos que armazenam dados sensíveis e confidenciais. Muitos escondem malwares que podem infectar seu computador, tablet ou celular.

• Mantenha o sistema operacional de seu computador, tablet ou celular sempre atualizado e, se possível, instale programas de antivírus.

• Ao acessar ambientes on-line que exijam login e senha, lembre-se de desmarcar o memorizador de senhas e sempre clique em Sair ao término de sua navegação.

• Instale aplicativos apenas de fontes confiáveis e lojas oficiais.

• Evite abrir e-mails e clicar em anexos ou links enviados por desconhecidos.

• Não confie em tudo o que ouvir ou ler; tenha cuidado ao compartilhar links.
A veiculação de notícias falsas é um grande meio para a prática de engenharia social.

• Se desconfiar de alguma solicitação, entre em contato diretamente com a central de atendimento oficial da instituição.

• Ao receber ofertas de produtos ou serviços, pesquise se os dados informados pelo atendente ou por e-mail são legítimos e idôneos.

• Fique atento ao endereço do remetente do e-mail. Empresas de grande porte não utilizam contas privadas como @gmail, @hotmail ou @terra para entrar em contato com seus clientes. Entidades públicas sempre são registradas com @gov.br ou @org. br.

• Ao criar um perfil em redes sociais, configure o controle de privacidade de suas publicações (somente para amigos ou para determinados grupos) e tenha cautela com o excesso de exposição virtual, pois as informações disponíveis podem atrair criminosos e colocar em risco a sua segurança e a de sua família.

• Em caso de perda, roubo ou furto de seu celular, solicite, o mais rápido possível, o bloqueio de seu chip na operadora de telefonia, bem como de seus cartões de crédito e de débito junto ao banco. Registre boletim de ocorrência na delegacia mais próxima.

• Sempre que não estiver utilizando seu celular, tablet ou computador, mantenha-os bloqueados com senha de acesso.

Dicas úteis para proteger informações corporativas

• Realize o controle de acesso de terceiros mediante registro e conferência de documento de identificação para ingresso nas dependências da empresa. Evite que visitantes tenham acesso a áreas restritas ou que detenham guarda de documentos.

• Para acesso à rede wi-fi, exija um cadastro prévio com informações pessoais.

• Mantenha gavetas fechadas e documentos importantes bem guardados.

• Retire imediatamente da impressora ou copiadora os documentos que não são para conhecimento público.

• Ao descartar documentos impressos ou materiais que contenham informações sensíveis, fragmente-os antes do descarte.

• Sempre configure senha para utilização e bloqueio em caso de ausência para seus celulares (pessoal e corporativo) .

• Não compartilhe login e senha de acesso com terceiros, mesmo que também sejam funcionários.

• Não esqueça de bloquear a tela do seu computador digitando Ctrl + Alt + Del ou de fazer o logout ao sair da mesa de trabalho.

• Desconfie de ligações que solicitam informações sobre procedimentos internos, rotinas e agendas de funcionários.

• Não forneça informações sobre a empresa, estrutura física, quadro de funcionários ou sobre rotinas, a menos que tenha certeza de que o solicitante é confiável.

• Evite publicar fotos do ambiente de trabalho em redes sociais.

• Fique atento a interesses exagerados de terceiros em informações corporativas.

• Evite descuidos ao falar sobre assuntos confidenciais corporativos ao telefone e em ambientes como elevador e hall de circulação.

• Instale as atualizações de software solicitadas e obedeça às políticas internas relacionadas à segurança da informação.

Fique atento e se proteja!

A conscientização e a prevenção são as formas mais efetivas para você não se tornar mais uma vítima de golpes.

FEBRABAN

Federação Brasileira de Bancos

Esta publicação foi baseada na Cartilha de Engenharia Social produzida pela FEBRABAN, FIESP E MNSP, em 2017, e foi revisada pelo Grupo de Trabalho de Conscientização da Comissão Executiva de Prevenção a Fraudes da FEBRABAN, em 2020.