GUIA DE ENGENHARIA SOCIAL

Como agir da forma correta

Índice

Por que as PMEs devem se preocupar com engenharia social

As pequenas e médias empresas estão cada vez mais cientes de que são alvos de cibercriminosos, de acordo com uma pesquisa de 2019 realizada pela Zogby Analytics, em nome da *US National Cyber Security Alliance*. Quase metade (44%) das empresas com 251 a 500 funcionários relataram ter sofrido uma violação de dados oficial nos últimos 12 meses. A pesquisa descobriu que 88% das pequenas empresas acreditam ser, pelo menos, um alvo "um pouco provável" para os cibercriminosos, incluindo quase metade (46%) que acredita ser um alvo "muito provável".

Os danos são reais e impactantes, um ponto muito bem ilustrado pelo relatório anual do Internet Crime Complaint Center (IC3), do FBI. Somente em 2020, o IC3 recebeu 19.369 reclamações de comprometimento de e-mails empresariais (BEC)/ comprometimento de contas de e-mail (EAC), com perdas ajustadas superando 1,8 bilhão de dólares. Para iniciantes, esses ataques BEC/EAC são um tipo de fraude sofisticada que visa empresas e indivíduos que realizam transferências de fundos.

Trinta e três por cento das violações incluíram ataques sociais, a segunda tática mais utilizada após hacking, segundo o Relatório de Investigações de Violação de Dados de 2019.

Após as PMEs sofrerem uma invasão

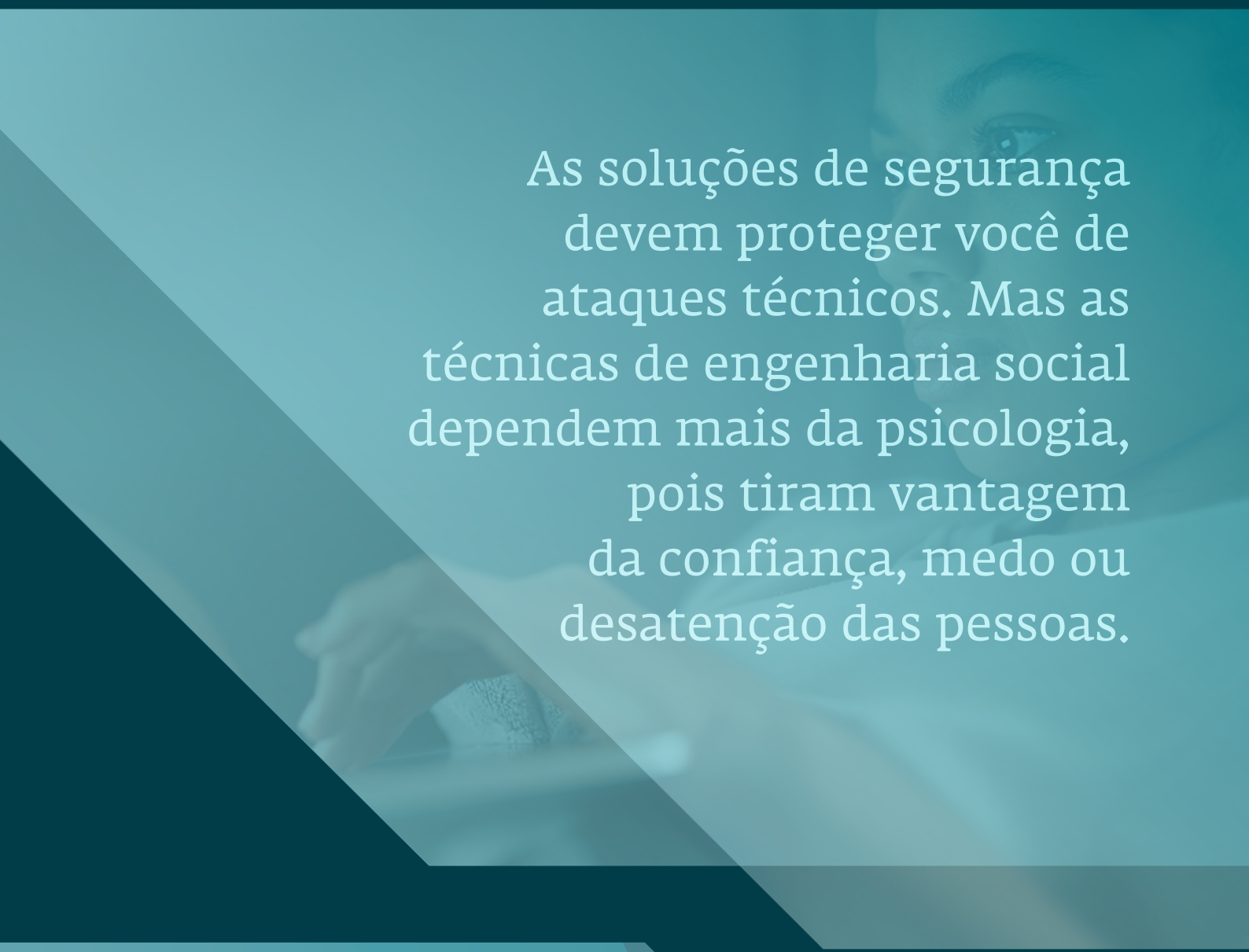
37%	25%	10%
tiveram perdas financeiras	entraram com pedido de falência	fecharam seu negócio

Fonte: NCSA

Introdução

O objetivo deste manual é ajudar a explicar a engenharia social e seus riscos para todos os funcionários da empresa. Nós somos seres levados pelas emoções, e a engenharia social é uma maneira muito eficaz de tirar proveito dessa característica. Além disso, os ataques de engenharia social geralmente não exigem habilidades técnicas altamente específicas por parte dos invasores. Forçar milhares de usuários a compartilharem informações confidenciais ou realizarem ações prejudiciais tem sido bastante fácil até agora! Não se deixe enganar: você pode, facilmente, tornar-se um alvo também.

Nas páginas a seguir, você encontrará uma visão geral das tendências em engenharia social, bem como exemplos dos tipos mais comuns de ataques que podem afetar as atividades on-line dos colaboradores. Você também aprenderá a reconhecer esses ataques, como proteger você e sua empresa deles.



As soluções de segurança devem proteger você de ataques técnicos. Mas as técnicas de engenharia social dependem mais da psicologia, pois tiram vantagem da confiança, medo ou desatenção das pessoas.

Técnicas de engenharia social

Spear phishing
Trata-se de uma forma direcionada de *phishing* que tem um indivíduo, organização ou empresa específica como alvo. As campanhas de phishing típicas não visam as vítimas individualmente – são enviadas para milhares de destinatários.

Vishing
Um método semelhante ao *phishing*, mas que emprega chamadas telefônicas fraudulentas em vez de e-mails. Os cibercriminosos geralmente se disfarçam de representantes de bancos ou seguradoras.

Smishing
Uma tentativa de engenharia social via mensagens de texto SMS. Na maioria das vezes, a tentativa de *smishing* visa redirecionar os destinatários para um site em que terão seus dados coletados. No entanto, também existem campanhas em que se solicita que as vítimas enviem dados confidenciais em uma resposta direta por SMS.

(S)extorsão
(S)extorsão é um esquema de golpe de e-mail de longa duração, que busca chantagear as vítimas usando alegações e acusações infundadas.

Personificação
A técnica de personificação é a mesma do mundo físico. Os cibercriminosos entram em contato com funcionários, geralmente se passando por seu CEO, tentando manipular as vítimas para que façam algo – ordenando e aprovando transações fraudulentas, por exemplo.

Scareware
Software que usa diversas técnicas geradoras de ansiedade para forçar as vítimas a instalarem códigos maliciosos em seus dispositivos. Por exemplo, um produto antivírus falso induz os usuários a instalarem um software específico para remover o problema, mas esse programa geralmente é prejudicial.

Golpe de suporte técnico
Os invasores tentam vender serviços falsos, remover problemas inexistentes ou instalar uma solução de acesso remoto nos dispositivos das vítimas para obter acesso não autorizado aos dados delas.

Phishing

Em algum momento de sua vida, é provável que você tenha vivenciado uma situação em que recebeu um e-mail supostamente enviado por um banco ou algum serviço on-line popular, solicitando a confirmação de suas credenciais ou número de cartão de crédito. Essa é uma técnica comum de *phishing*. Contudo, as armadilhas de *phishing* mudam constantemente – e, às vezes, são difíceis de reconhecer.

Phishing é uma forma de ataque de engenharia social em que o invasor tenta obter acesso a credenciais de login ou informações confidenciais, ou implementa ações de malware.
As campanhas de ***phishing*** podem segmentar um grande número de usuários anônimos, uma vítima específica ou um pequeno grupo de vítimas associadas com golpes personalizados (***spear phishing***). Ataques focados em indivíduos de negócios específicos, principalmente de alto perfil – como gerentes ou proprietários – são rotulados como "caça às baleias" (os criminosos que perseguem "o peixe grande").

Os cibercriminosos já sabem que há uma grande chance de e-mails serem verificados quanto a conteúdo malicioso pelo seu provedor de e-mail, encaminhando-os para uma pasta de lixo eletrônico. É por isso que o conteúdo das mensagens fraudulentas muda com tanta frequência.

Segundo o Google, os golpistas enviaram 18 milhões de e-mails de phishing sobre a covid-19 para usuários do Gmail todos os dias, em março de 2020.

Phishing

Desde que a pandemia de covid-19 foi deflagrada, os cibercriminosos não perderam tempo em tentar lucrar com a incerteza, o medo e a escassez de suprimentos relacionados à crise sanitária. Em março de 2020, houve uma enxurrada de spams com o tema covid-19, espalhando ***malwares***, realizando ações de ***phishing*** para obter informações confidenciais ou oferecendo produtos falsos, conforme revelado no relatório de ameaças da ESET do primeiro trimestre de 2020.

Não é surpresa que a pandemia tenha se tornado uma das principais iscas usadas pelos invasores. O surgimento de qualquer crise é sempre acompanhado de novas circunstâncias, que proporcionam um ambiente ideal para os cibercriminosos inovarem.

Noventa e quatro por cento dos malwares são entregues por e-mail.

17.700 dólares são perdidos a cada minuto devido a ataques de *phishing*.

Cerca de 14,5 bilhões de e-mails de spam são enviados todos os dias.

Fontes: CSO, hostingtribunal.com

Características básicas de phishing

1 Caso você não conheça o endereço de e-mail remetente, tome cuidado com os conteúdos recebidos.

2 Tenha sempre um pé atrás com arquivos anexados ou links desconhecidos. Eles podem conter um malware ou direcionar você a um site malicioso.

3 Assustador demais ou bom demais para ser verdade? Muito provável que seja golpe. Lembre-se de que a engenharia social se concentra nas fraquezas humanas.

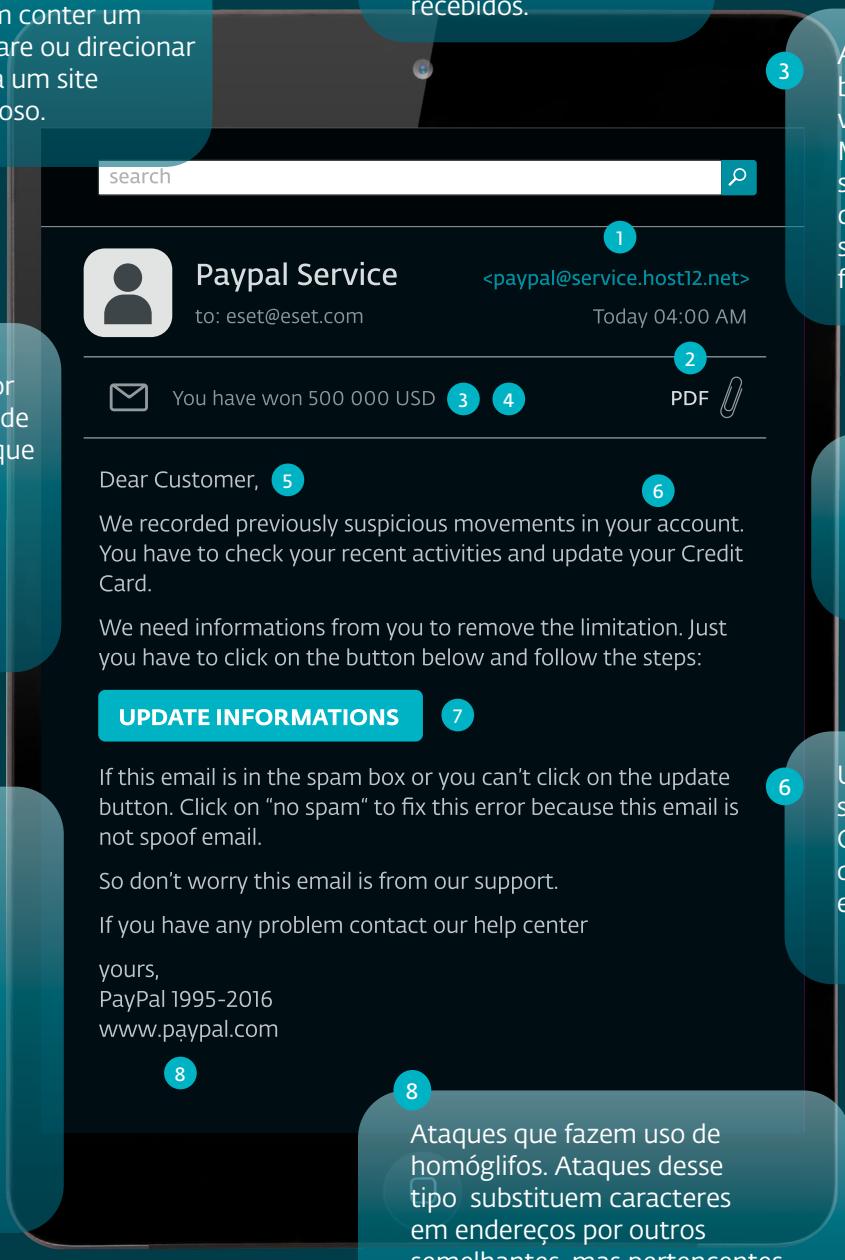
4 O assunto difere da mensagem.

5 Se a saudação for geral demais, pode ser um sinal de que não foi enviada apenas a você, como também a muitas outras pessoas.

6 Urgência suspeita? O golpista quer que você entre em pânico.

7 Erros de ortografia e outros erros gramaticais são comuns em e-mails de phishing que foram traduzidos de outros idiomas.

8 Ataques que fazem uso de homóglifos. Ataques desse tipo substituem caracteres em endereços por outros semelhantes, mas pertencentes a alfabetos diferentes (como "ạ" vs "a" em paypal.com).



Smishing

Smishing é um tipo de phishing que utiliza o serviço de mensagens de texto ou SMS. Esse método também se espalhou rapidamente durante os primeiros meses da pandemia de covid-19. Em épocas de incerteza, por exemplo, as pessoas começaram a receber mensagens SMS em que os remetentes se passavam por entidades oficiais dos governos locais.

O objetivo desses ataques é semelhante ao de phishing – os cibercriminosos podem **tentar obter seus dados pessoais ou forçam você a clicar em um link para um site malicioso**. Outra técnica baseia-se em nossa compaixão. Os cibercriminosos enviam mensagens de texto com um pedido de doação para pessoas em situações desesperadoras, como um fundo para vítimas de desastres de furacões ou outro tipo de caridade, geralmente pedindo informações de seu cartão de crédito.

No início, foi uma surpresa para muitas pessoas que os hackers pudessem obter seus números de telefone sem elas saberem. Mas, como muitos especialistas em segurança cibernética apontaram, **é mais fácil obter o número de telefone de alguém do que seu e-mail, porque há um número finito de opções para números de telefone**. Adivinhar os nomes dos endereços de e-mail é mais difícil justamente por permitirem mais caracteres.

Você consegue identificar por que esta SMS é suspeita?

Um banco nunca enviaria um link direto como este. Caso não tenha certeza, utilize seu banco on-line e verifique se recebeu a mesma mensagem pelo sistema. É sempre mais seguro navegar em um site oficial do que clicar em um link suspeito.

Vishing

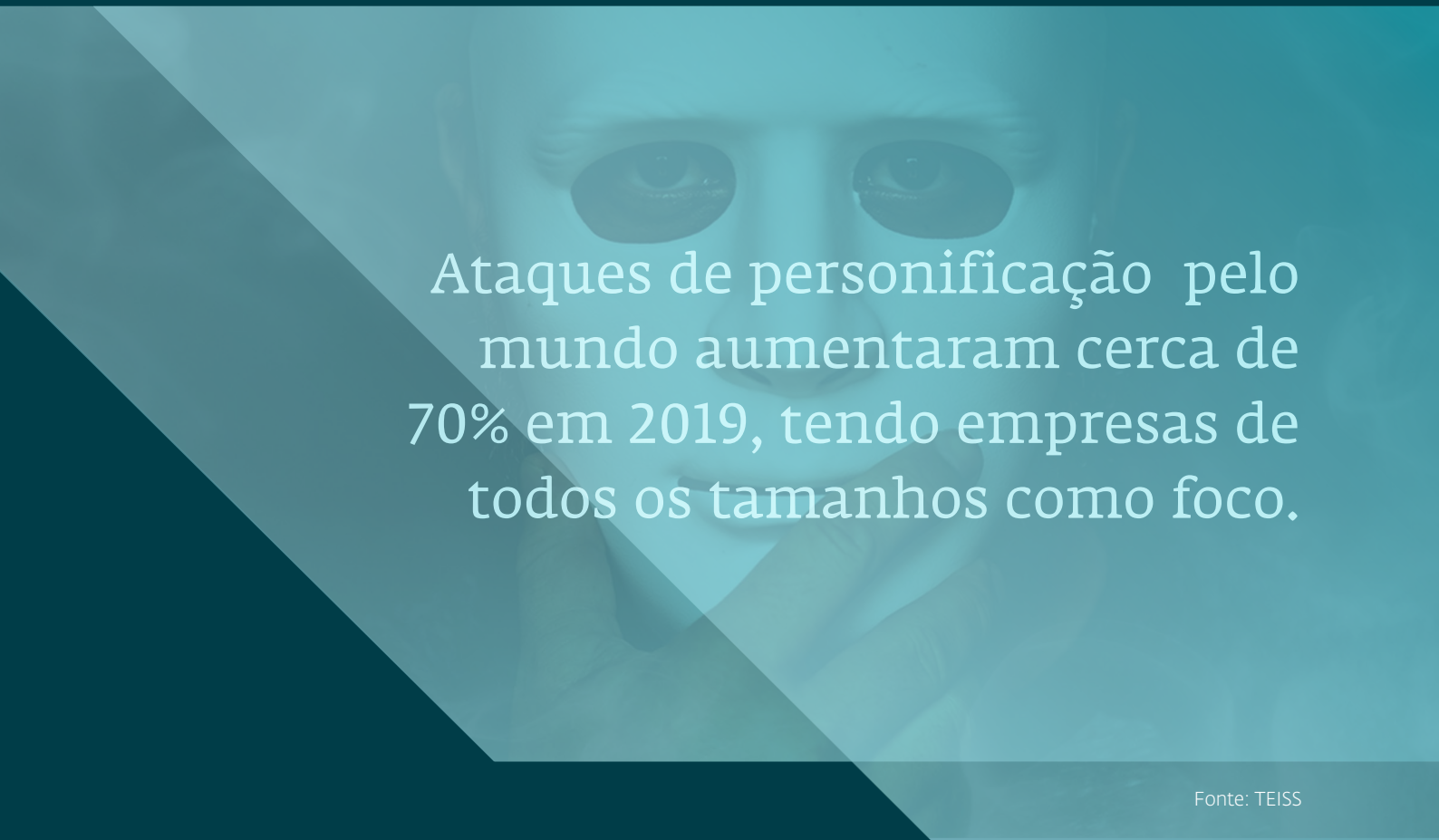
Vishing requer habilidades práticas ainda maiores do que outros tipos de golpes. Geralmente, ocorre assim: Um golpista liga para você e **finge ser um representante de uma instituição oficial**. O próximo passo é informar-lhe sobre uma conta bancária comprometida ou uma oferta de empréstimo não solicitada na tentativa de obter suas informações pessoais e dados financeiros. Ruim demais ou bom demais para ser verdade? Peça mais detalhes e **não compartilhe dados confidenciais imediatamente**. Outra opção é encerrar a chamada e entrar em contato com o atendimento ao cliente do seu banco e explicar o ocorrido.

Personificação: quando um invasor se passa por CEO

Vamos falar de personificação, mais um método de ataque não técnico usado pelos cibercriminosos para se passarem por pessoas confiáveis enquanto tentam manipular outras pessoas. Ao receber um contato, como diferenciar um cibercriminoso de seu colega?

A personificação é definida como a prática de fingir ser outra pessoa – nesse caso, **para obter informações ou acesso a uma pessoa, empresa ou sistema informático**. Para atingir esses objetivos, os cibercriminosos usam telefonemas, e-mails ou aplicativos de mensagens, entre outros métodos. Em muitos casos, os invasores escolhem nomes da alta administração da empresa e configuram um e-mail que parece ter sido escrito por um gerente.

É inacreditável a quantidade de informações corporativas disponíveis em plataformas como o LinkedIn que divulgam a estrutura da empresa e os nomes de seus funcionários.
Um invasor pode usar esses dados para tentar entrar em contato com vários funcionários da empresa, **solicitando que façam transferências de dinheiro, paguem faturas ou enviem dados importantes**.
É por isso que a personificação pode ser tão perigosa para as empresas – esses ataques podem causar uma violação de dados e perdas financeiras.

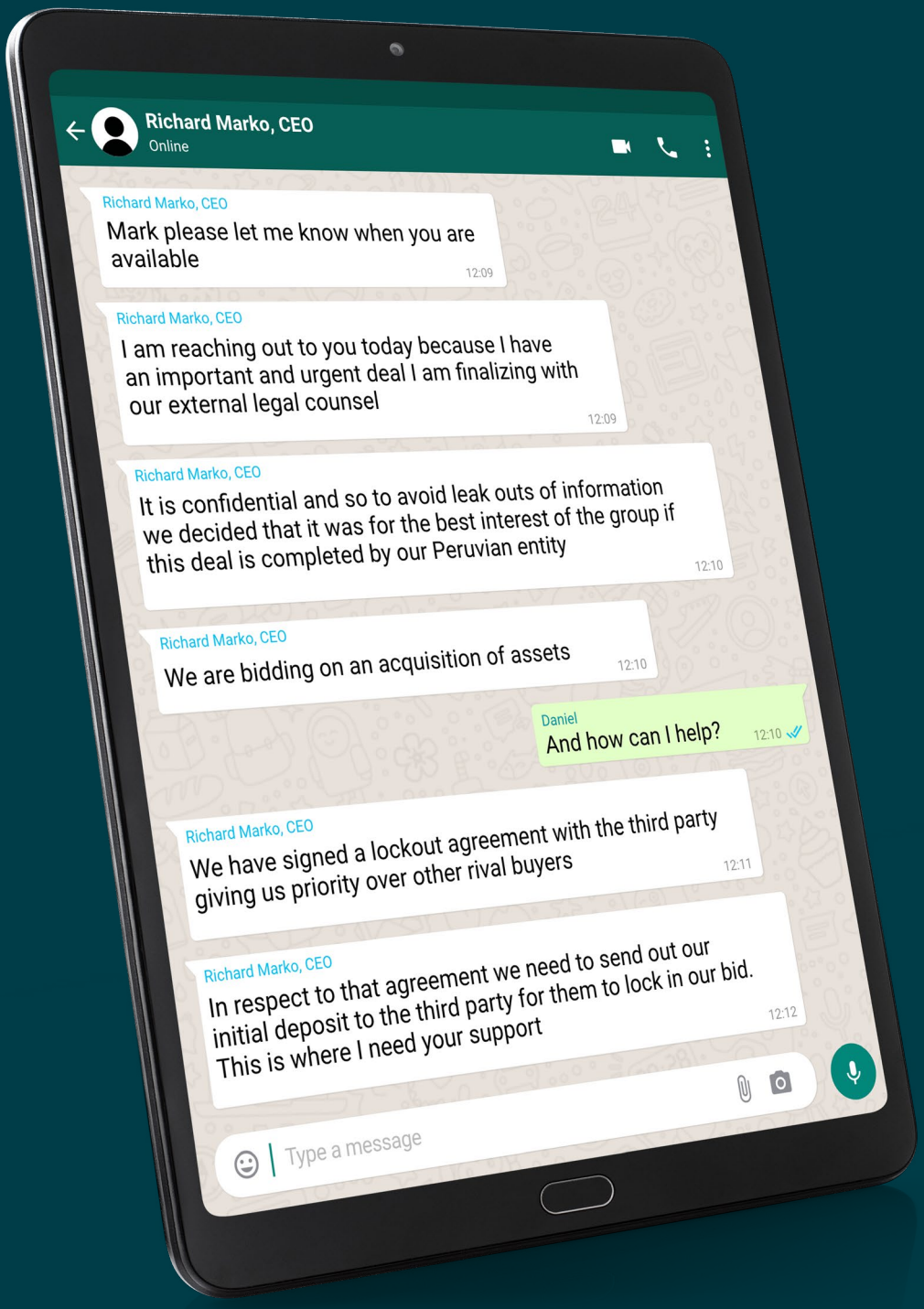


Ataques de personificação pelo mundo aumentaram cerca de 70% em 2019, tendo empresas de todos os tamanhos como foco.

Fonte: TEISS

História real: ataque de personificação contra a ESET

Ciberataques podem acontecer em qualquer organização. Em 2020, a ESET enfrentou tentativas de personificação de CEO por meio de mensagens do WhatsApp. O objetivo dessas tentativas era falsificar a existência de um grande lance, que exigia um depósito financeiro.



Como contornar ataques de personificação

Lembre-se, estar consciente deles é o segredo. Quanto mais sabemos sobre ataques de personificação, mais conseguimos evitá-los. Vejamos como os e-mails de personificação funcionam. Muitos tentam incutir um senso de urgência e medo em seus alvos. Esse sentimento leva as vítimas a realizarem a tarefa desejada, que pode envolver algo que você considera incomum e suspeito, como compras que não estão relacionadas ao seu negócio, com clientes que você não reconhece. Os cibercriminosos também tentam impor um prazo curto para finalizar as ações solicitadas.

Mensagens fraudulentas geralmente contêm erros gramaticais ou usos incorretos da marca corporativa. No entanto, esses são apenas os aspectos mais fáceis de detectar. Os invasores adeptos da personificação avançada podem fabricar uma mensagem de e-mail que pareça muito real, incluindo uma foto ou assinatura oficial de um funcionário ao fim de um e-mail. Portanto, mesmo que o modelo pareça legítimo, tenha cuidado caso a solicitação da mensagem parecer estranha.

CONSIDERE O CONTEXTO

Às vezes, estamos muito ocupados e tomamos decisões sem pensar duas vezes. Talvez demore alguns segundos a mais, mas sempre considere se o e-mail faz sentido. Por que razões esse(a) colega estaria fazendo apenas esse pedido de compra ou essa informação pessoal confidencial? **Qualquer detalhe incomum e que se desvie dos procedimentos rotineiros deve ser um sinal de alerta**. Mesmo que o e-mail aparentemente venha de uma pessoa confiável, como o CEO, pode ser uma fraude. Fique atento(a) e verifique quaisquer solicitações com outros colegas.

FORA DO ESCRITÓRIO?

É possível que os cibercriminosos saibam quando alguém está fora do escritório e finjam ser essa pessoa. Nesse caso, verifique as informações com seu superior ou colegas de trabalho. Como diz o ditado, é melhor prevenir do que remediar.

Como contornar ataques de personificação

VERIFIQUE O ENDEREÇO DE E-MAIL

Recebeu um e-mail comercial de uma conta pessoal? Aparentemente, o endereço de e-mail pode pertencer a alguém que você conhece. Mas é sempre melhor responder a essa pessoa em seu endereço de e-mail oficial. Além disso, às vezes, os invasores podem usar um e-mail que parece quase um endereço corporativo oficial com um mero detalhe diferente, como substituir "m" por "rn".

Implemente a tag "EXTERNO"

Em uma mudança recente da segurança interna da ESET, e-mails vindos de fora do domínio da empresa são sempre marcados como EXTERNO. Isso não ajudaria caso o impostor do CEO estivesse fingindo enviar o e-mail do e-mail privado do CEO, mas poderia ajudar a identificar e-mails tentando falsificar o domínio (como o caso "m" e "rn").

CONFIRME QUE SE TRATA DA PESSOA EM QUESTÃO POR OUTRO CANAL DE COMUNICAÇÃO

Se você recebeu uma mensagem suspeita no WhatsApp, escreva para a pessoa por meio de um e-mail corporativo ou ligue para ela. Outra opção é simplesmente **perguntar diretamente à pessoa, cara a cara.** Não se preocupe em incomodar alguém, mesmo se a pessoa estiver ocupada. Por exemplo, você pode se sentir relutante em incomodar um(a) CEO. Isso é natural, porque quanto mais alta a posição de um colega, mais hesitamos em entre em contato com eles, especialmente quando estiverem fora do escritório.

Nesse caso, **considere consultar outro colega ou superior**. Por exemplo, um grande e urgente pagamento de fatura em atraso certamente seria (ou deveria) ser conhecido pelo seu CFO ou COO, então verifique com eles. Lembre-se – todo cuidado é pouco.

"Oi, meu amigo. Você não me conhece, mas eu te conheço muito bem. Melhor do que você imagina. Esta é sua senha, certo?"

E-mails como este podem aparecer na caixa de correio de qualquer pessoa. O chantagista misterioso geralmente afirma ter perseguido o destinatário por meio de sua webcam enquanto assistia a algum conteúdo adulto, forçando o destinatário a pagar para se livrar do problema para que sua família e colegas de trabalho não saibam do ocorrido (sextorsão). Para provar que eles realmente invadiram o computador da pessoa, informam uma senha que a vítima usa. Mas os golpes de (s)extorsão costumam ser fraudes.

VIVEMOS NA IDADE DE OURO DE GOLPES DE (S)EXTORSÃO

Um exemplo recente de como os hackers fazem mau uso da tecnologia e de uma crise para espalhar golpes é a pandemia de covid-19. À medida que muitas empresas mudaram para o trabalho remoto e escritórios em casa, onde os funcionários não estavam protegidos pela rede corporativa, o número de ameaças on-line aumentou. Os cibercriminosos, por exemplo, ameaçaram infectar a vítima e sua família com coronavírus caso não pagassem.

Ao pagar a quantia exigida, você só perde dinheiro e abastece os negócios dos criminosos, ajudando-os a espalhar mais golpes.

ENTENDA O QUE O CRIMINOSO QUER

Tenha em mente que o principal objetivo dos e-mails de (s)extorsão é fazer você pagar alguma quantia – preferencialmente em Bitcoins, o que permite que os hackers recebam o dinheiro anonimamente. Golpes são um ótimo negócio: de acordo com o Internet Crime Complaint Center do FBI, a (s)extorsão por e-mail causou perdas de cerca de 70,9 milhões de dólares em 2020.

SAIBA COMO REAGIR A GOLPES DE (S)EXTORSÃO

Não envie dinheiro, nem responda ou clique em links ou anexos. Se você for vítima de um golpe de (s)extorsão, sempre informe a equipe de TI da empresa ou os departamentos de segurança internos. E, se possível em seu país, o incidente deve ser relatado (se você for do Reino Unido, por exemplo, relate-o on-line ao centro Action Fraud; nos Estados Unidos, faça uma queixa junto ao site do FBI).

A melhor prevenção é criar uma senha ou frase secreta forte. Além disso, o negócio de venda de senhas é o motivo pelo qual todos precisam alterar suas senhas de vez em quando ou devem usar fatores de proteção adicionais (autenticação multifator).

SE A SENHA ESTIVER CORRETA, NÃO ENTRE EM PÂNICO

Mencionar uma senha real é apenas mais uma técnica para deixar o destinatário nervoso. Os invasores podem saber sua senha, mas provavelmente é tudo o que eles têm. É provável que a tenham comprado na dark web ou a tenham descoberto após vazamento em uma violação de dados.

NÃO SUBESTIME OS DESAFIOS DE SEGURANÇA DO TRABALHO REMOTO

Locais de trabalho e escritórios flexíveis são ótimos, mas somente se estiverem bem protegidos e você souber como lidar com eles. As redes Wi-Fi são altamente propensas a ataques. Portanto, se você quiser ter certeza de que a conexão e os dados da empresa estão seguros, busque utilizar uma conexão VPN, que permite estabelecer uma conexão segura à rede da empresa.

Como os hackers invadem seu computador e sua webcam?

Os golpes de (s)extorsão não causarão nenhum dano caso você os gerencie atentamente. Ainda assim, lembre-se de que existe uma maneira de os hackers entrarem na sua webcam. Eles costumam usar malwares, como um Trojan (cavalo), para infectar seu dispositivo com software de desktop remoto – mas, para isso, precisam de sua ajuda. Às vezes, basta baixar algum software desconhecido. Embora você pense que conseguiu o que queria, pode haver algum malware oculto no arquivo. Sem saber, você acabou de ajudar os hackers a infectarem seu dispositivo. E não espere que a luz da webcam acenda assim que eles começarem a investigar sua vida on-line. Se acendesse, eles não permaneceriam imperceptíveis, correto?

Se o seu computador estiver infectado, os invasores podem não apenas ver os momentos íntimos de sua vida, mas também capturar dados e documentos confidenciais ou gravar suas conversas se também tiverem hackeado seu microfone.

Como reagir a uma mensagem de (s)extorsão

1. Aja de forma cautelosa e cuidadosa, evitando ações precipitadas.
Os criminosos por trás dos esquemas de (s)extorsão visam as fraquezas humanas e tentam manipular as pessoas para prejudicá-las. Portanto, se você receber uma mensagem que gere medo, pare e considere a possibilidade de que nada no e-mail seja verdade. Se você não tiver certeza, sempre consulte o departamento de TI ou o suporte técnico do provedor de segurança.

2. Não pague nada aos (s) extorsionistas.
E-mails de (s)extorsão geralmente são apenas golpes. Isso significa que não há os cibercriminosos não possuem o que alegam; não devem ter nenhum vídeo seu ou o que você assistiu, não são nenhuma autoridade oficial, tampouco ordenaram um ataque contra você.

3. Não interaja com o e-mail, de nenhuma maneira.
Não responda ao golpe, não baixe seus anexos e não clique em links incorporados ou interaja com qualquer conteúdo, pois esses elementos podem levar a malwares ou outras ameaças.

4. Verifique/altere sua senha.
Em alguns casos, os criminosos testam as credenciais vazadas e, se forem bem-sucedidos, usam a conta hackeada pelo menos para divulgar suas mensagens. Portanto, se um invasor listar qualquer uma de suas senhas reais, altere-as imediatamente e ative a autenticação multifator para aumentar sua proteção.

5. Encaminhe o e-mail ao departamento de TI.
Se sua empresa não possuir uma equipe de TI, o mínimo que você pode fazer é escanear o computador e a rede com uma solução de segurança confiável e se certificar de que nenhuma de suas senhas foi vazada ou comprometida.

6. Proteja sua webcam.
Para evitar um possível uso indevido da sua webcam de fábrica, use software de proteção ou pelo menos coloque um pedaço de fita sobre a câmera. Dessa forma, você terá certeza de que os criminosos não têm como gravar um vídeo seu sentado na frente dos dispositivos.

7. Use uma solução antispam.
Use uma solução antispam. Uma solução de segurança confiável com funcionalidade antispam pode ajudar a impedir que golpes de (s)extorsão cheguem à sua caixa de entrada no futuro.

Outras técnicas de engenharia social que você deve conhecer

Scareware é um tipo de *malware* que tenta induzir as vítimas a comprarem e baixarem softwares potencialmente perigosos. É um método que rapidamente atrai a atenção das pessoas. Mas também as assusta. Anúncios pop-up difíceis de fechar, empresas de software com nomes que você nunca ouviu falar e verificação não autorizada de vírus em seu computador – todos esses são atributos típicos de scareware.

O problema é que esses programas geralmente exibem uma lista de dezenas ou centenas de vírus falsos. Mas os programas de scareware não estão escaneando seu computador, e esses resultados supostamente descobertos são falsos. Os avisos sobre uma detecção perigosa apenas manipulam suas ações para que você realmente faça o download de uma infecção. Esses golpes geralmente se baseiam em softwares de segurança falsos, como Advanced Cleaner, SpyWiper ou System Defender.

Escolha produtos de software conhecidos, testados e atualizados

Assim, você saberá que um convite para baixar um software gratuito deve ser um golpe. Também é muito útil usar bloqueadores de pop-up em seus dispositivos de trabalho e filtros de URL. Estabeleça ferramentas de segurança on-line e firewalls para impedir os invasores de chegarem até você.

Golpes de suporte técnico estão intimamente relacionados ao scareware. Mas, ao contrário do scareware, eles fingem ser de uma empresa renomada, como a Microsoft. Eles não começarão a escanear seu computador automaticamente. Em vez disso, podem pedir para você abrir alguns arquivos – e então dizer que esses arquivos mostram um problema... que não existe.
De acordo com a Comissão Federal de Comércio dos EUA (FTC), os golpes de suporte técnico não são incomuns. Em 2019, a FTC recebeu mais de 100 mil denúncias desse tipo de golpe.

Checklist para administradores de TI:
5 maneiras de proteger sua empresa de ataques de engenharia social

1. Ofereça treinamento regular de segurança cibernética de todos os funcionários, incluindo a alta administração e a equipe de TI. Lembre-se de que esse treinamento deve mostrar ou simular cenários da vida real. Os pontos de aprendizado devem ser acionáveis e, acima de tudo, testados ativamente fora da sala de treinamento.

2. Procure por senhas fracas que possam se tornar uma porta aberta na rede da sua organização para invasores. Além disso, proteja as senhas com outra camada de segurança implementando autenticação multifator.

3. Implemente soluções técnicas para lidar com comunicações fraudulentas para que mensagens de spam e phishing sejam detectadas, colocadas em quarentena, neutralizadas e excluídas. As soluções de segurança, incluindo muitas oferecidas pela ESET , possuem alguns ou todos esses recursos.

4. Crie políticas de segurança compreensíveis, que os funcionários possam usar e que os ajudem a identificar quais etapas precisam seguir em casos de engenharia social.

5. Use uma solução de segurança e ferramentas administrativas, como o ESET PROTECT Console, para proteger os endpoints e as redes da sua empresa, dando aos administradores visibilidade total e a capacidade de detectar e mitigar ameaças potenciais na rede.

Por mais de 30 anos, a ESET® vem desenvolvendo softwares de segurança líder do setor para empresas e consumidores em todo o mundo. Com soluções de segurança que vão desde defesa móvel e de endpoints até criptografia e autenticação

multifator, os produtos de alto desempenho e fácil uso da ESET dão aos usuários e empresas a tranquilidade para aproveitarem todo o potencial de sua tecnologia. A ESET protege e monitora discretamente 24 horas por dia, 7 dias por semana,

atualizando as defesas em tempo real para manter os usuários seguros e os negócios funcionando ininterruptamente. Para mais informações, visite www.eset.com.