ESTRADA PARA O FUTURO

CIBERSEGURANÇA NO DIA A DIA

Entenda os golpes cibernéticos e saiba quais medidas tomar para uma postura eficiente de segurança

Se você já caiu em um golpe, conhece bem o sentimento de ter sido enganado. Talvez fosse tarde e você estivesse lutando contra o cansaço, ou estivesse com pressa. Talvez tenha recebido um e-mail alarmante sobre um problema com seu salário, sua conta de telefone celular ou seus impostos.

Seja qual for a razão, você reagiu clicando em um link suspeito ou dando informações pessoais antes de perceber que se tratava de um golpe cibernético.

Você não está sozinho. Em uma pesquisa recente realizada pela empresa Tessian, 43% das pessoas admitiram ter cometido um erro no trabalho que teve repercussões de segurança, enquanto quase metade (47%) das pessoas que trabalham na indústria de tecnologia disseram ter clicado em um e-mail de phishing no trabalho.

FACILITAMOS O TRABALHO DO CRIMINOSO CIBERNÉTICO QUANDO SUBESTIMAMOS O RISCO

A maioria das violações de dados ocorrem por causa de erros humanos. Os hackers estão cientes disso e sabem que, no geral, não somos bons em perceber quando estamos sendo enganados. Nosso excesso de confiança em nossa capacidade de discernimento nos atrapalha.

Em outras palavras, acabamos caindo em golpes justamente por acharmos que jamais cairíamos.

Se está trabalhando em casa, uma pessoa pode confiar que o empregador está cuidando da segurança cibernética para ela. Ou usar um sistema gratuito de bloqueio de anúncios, sem perceber que ele não impede downloads de malware. Ou, talvez, ainda acredite no mito de que computadores da Apple não pegam vírus (eles pegam).

Da mesma forma que você não deixa sua carteira e telefone por aí, você sempre precisa estar pelo menos parcialmente ciente da segurança do computador. Preste atenção e trate tudo – e-mails, sites, downloads de software – com um grau saudável de suspeita. Fazer isso o faz bem preparado para bloquear muitos ataques comuns.

GOLPES ENVOLVEM TRUQUES PSICOLÓGICOS

Entre os truques preferidos dos cibercriminosos, está aquele que usa o nosso medo de perder uma oportunidade que outras pessoas estão aproveitando. Pode ser uma chance de negócio imperdível, por exemplo, do tipo que
pouca gente conhece. O e-mail ou o link darão a entender que a vítima precisa correr enquanto o acesso àquela oportunidade ainda é privilegiado.

Assim, os criminosos cibernéticos criam um senso de urgência, induzindo as pessoas a agirem antes de pensar.

FAZ PARTE DOS GOLPES IR GANHANDO A CONFIANÇA DA VÍTIMA AOS POUCOS

Se alguém te mandar um e-mail perguntando, de cara, seu número e senha do cartão, você não vai responder, certo?

Por isso é que um cibercriminoso inteligente irá começar se passando por uma instituição conhecida, fazendo perguntas inofensivas. Vai ganhar a confiança da vítima aos poucos, com carisma, reciprocidade e uma abordagem amigável.

Importante lembrar que tempos difíceis nos tornam mais vulneráveis. Situações como desemprego em alta, pandemias e inadimplência são condições ideais para fraudadores.

Cibercriminosos irão usar promessas falsas nas quais queremos desesperadamente acreditar. E nos induzir a clicar em links, preencher formulários falsos, acessar aplicativos fraudulentos e passar dados sigilosos.

Os hackers modernos podem encontrar tudo o que precisam saber sobre um alvo em potencial através do Google ou mídias sociais. E usar essas informações para arquitetar o golpe perfeito, com o objetivo de atrair as pessoas a baixar um malware, enviar dinheiro, compartilhar informações sigilosas ou divulgar detalhes de login.

QUAIS MEDIDAS TOMAR?

Tente pesquisar seu nome ou criar uma segunda conta de mídia social para ver seus próprios perfis, como um estranho faria

Você está confortável com tudo o que vê? Se não, defina suas contas sociais para sigilos privados e verifique se você realmente conhece todos os seus seguidores.

Não reutilize senhas

De acordo com pesquisas, 85% das pessoas reutilizam senhas. Não seja uma delas. Criminosos costumam testar em várias contas de um usuário uma mesma senha roubada. Um gerenciador de senha pode ajudar no trabalho de gerar e guardar chaves diferentes e mais fortes.

Tenha autenticação multifatorial no login

Habilite a autenticação multifatorial (MFA) para garantir que a única pessoa que tenha acesso à sua conta seja você. Use-o para e-mail, bancos, mídias sociais e qualquer outro serviço que exija login. Para habilitar a autenticação multifatorial, use um dispositivo móvel confiável, como seu smartphone, ou um aplicativo autenticador.

Seja cético quanto aos e-mails pessoais e de trabalho

Se a mensagem parecer estranha, clique no nome de exibição do remetente para garantir que o endereço de e-mail corresponde ao legítimo. Em caso de pedidos para clicar em links, ou executar tarefas que envolvam dados sigilosos, peça uma segunda opinião da equipe de TI da empresa. Se o remetente for de um colega, procure-o e confirme verbalmente se ele enviou realmente o e-mail.

Se você recebeu uma mensagem inesperada ou incomum, ignore. Por mais urgente que pareça. O senso de urgência é uma das principais armas dos golpistas, porque tira o seu tempo de pensar.

TRÊS TÁTICAS PERSUASIVAS COMUNS EM GOLPES DE PHISHING

1 Apelos de uma autoridade percebida:

(“Atualização da política de férias”);

2 Ofertas de ganho financeiro:

(“Ganhe dinheiro em casa!”);

3 Problemas de segurança do usuário:

(“Tentativa de acesso à sua conta”).

Mantenha-se protegido enquanto estiver conectado no Wi-Fi

Sempre que você está online, você está vulnerável. Pratique navegação segura na Web onde quer que você esteja, verificando o ícone de "bloqueio verde" ou cadeado na barra do navegador. Evite acesso gratuito à internet sem criptografia. Se você usar um ponto de acesso público inseguro, evite atividades sensíveis, que requerem senhas ou cartões de crédito.

Fique de olho em seus aplicativos

Seu dispositivo móvel pode estar cheio de aplicativos suspeitos em execução em segundo plano ou usando permissões padrão que você nunca percebeu que aprovou — coletando suas informações pessoais sem o seu conhecimento. Verifique as permissões do seu aplicativo e use o princípio do menor privilégio, que parte da premissa de fornecer somente as permissões necessárias. Apenas baixe aplicativos de fontes confiáveis.

Não confie em tudo o que chega pelo WhatsApp

As pessoas tendem a acreditar que tudo o que chega por aplicativos de mensagem é legítimo, já que os contatos normalmente são conhecidos. Suspeite de pedidos de dinheiro e de links de notícias enviados repentinamente.

Abandone as versões gratuitas de antivírus

A decisão de pagar por um antivírus não pode partir dos recursos que uma versão gratuita oferece, e sim de como uma pessoa interage com o mundo online, e o quanto ela tem a perder caso tenha o computador invadido. As soluções pagas tendem a oferecer um conjunto completo de ferramentas e recursos em um pacote, com uma gama muito mais ampla de proteção. Além disso, há um time de suporte à disposição. E o antivírus pago vai entregar uma gestão centralizada de todos os dispositivos, incluindo os móveis, como celulares e tablets.

Pare o compartilhamento excessivo

Todos parecem estar postando suas informações nas mídias sociais — desde endereços pessoais até onde gostam de tomar café. Detalhes úteis para criminosos atingirem você, seus entes queridos e até mesmo seu dinheiro. Evite postar nomes, números de telefone, endereços, locais de escola e trabalho e outras informações confidenciais (seja na legenda ou na foto que tirou). Desabilite o geotagging, que permite que qualquer pessoa veja onde você está — e onde você não está — em qualquer momento.

Se você se conectar, você deve proteger seu dispositivo

Uma vez que seu dispositivo se conecta ao mundo digital, torna-se vulnerável a todos os tipos de riscos. Seja seu computador, smartphone, dispositivo de jogo ou outros dispositivos de rede, a melhor defesa é atualizá-los com os mais recentes softwares de segurança, navegadores da Web e sistemas operacionais. Se puder, ative as atualizações automáticas. Tenha um software antivírus em cada um dos seus dispositivos. E, ao usar um USB para um disco rígido externo, certifique-se de que o software de segurança procurou por vírus e malwares.

Converse com seus filhos sobre a internet

Ensine-os sobre o uso responsável da internet sem desligar os canais de comunicação. Certifique-se de que eles saibam que podem vir até você se estiverem sofrendo qualquer tipo de assédio online, perseguição ou bullying.

Evite sites que oferecem download de vários programas diferentes

Se você precisa baixar um software, vá até o site oficial. Fuja de sites informais.

Instale o mínimo possível de extensões de navegador

Seu navegador pode ser incrementado com uma série de aprimoramentos conhecidos como extensões e complementos. E como qualquer software que você baixa, essas extensões podem apresentar problemas para a segurança do seu navegador e, consequentemente, de seus arquivos.

MANTENHA UMA MENTALIDADE DE CIBERSEGURANÇA

A lógica de proteção é simples:

- Se algo parece bom demais para ser verdade, muitas vezes é porque de fato não é verdade;
- Nenhuma oportunidade é tão urgente que não mereça uma investigação prévia;
- Pare e pense antes de abrir anexos, clicar em links ou compartilhar informações por e-mail. Até segunda ordem, tudo pode ser golpe ou vírus.

ESTRADA PARA O FUTURO

QUER SABER MAIS A RESPEITO DE SEGURANÇA CIBERNÉTICA?

ACESSE

ISH.COM.BR/BLOG/

EMPRESA CERTIFICADA

ISO9001 | ISO20000 | ISO27001