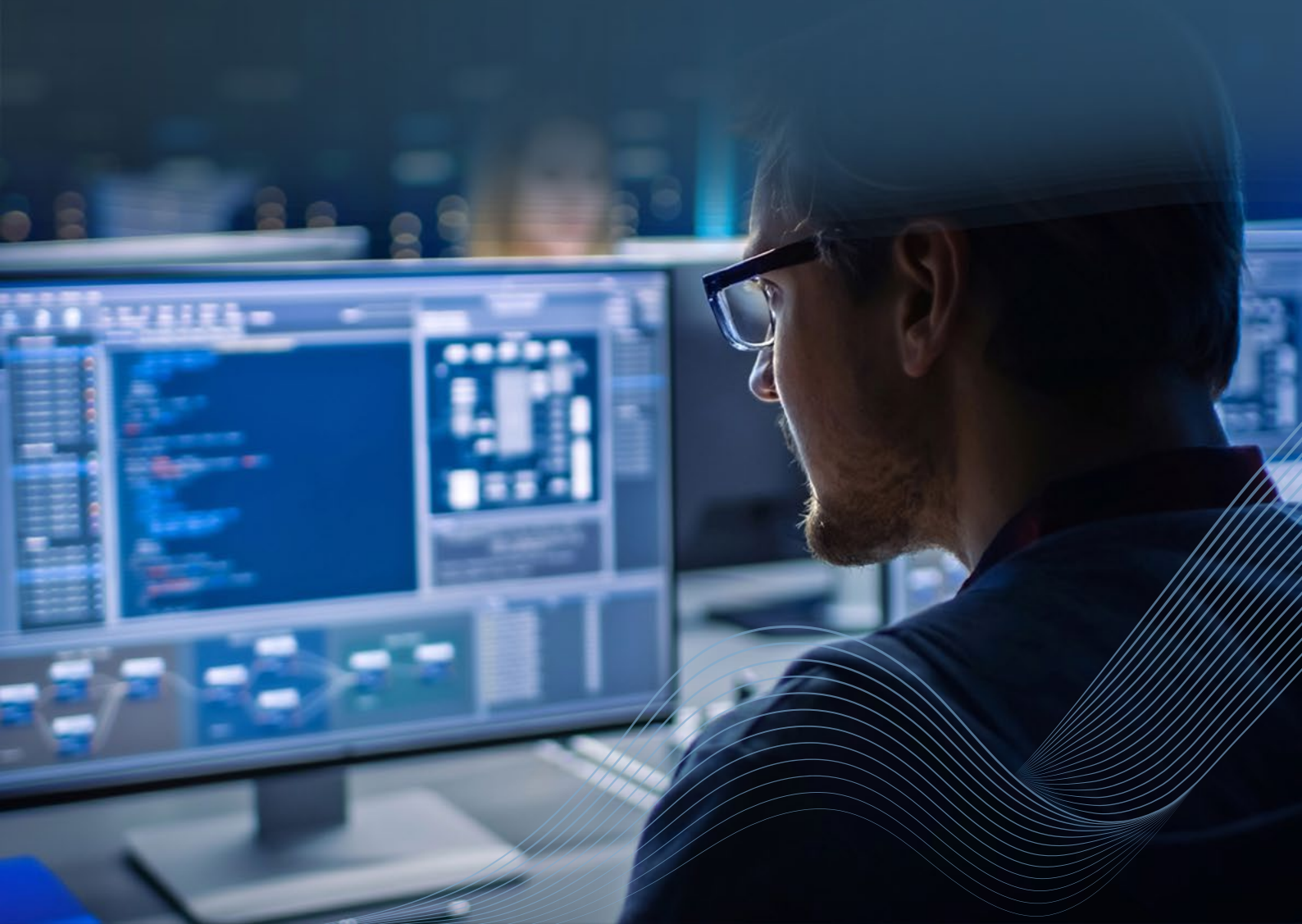
ESTRADA PARA O FUTURO

MANUAL DE CIBERSEGURANÇA PARA EXECUTIVOS

Protegendo informações sigilosas no C-level



ESTRADA PARA O FUTURO

Executivos do C-level têm 12 vezes mais chances de serem alvo de ataques cibernéticos na comparação com outros funcionários da organização. Os motivos são o constante acesso a informações privilegiadas, com menos restrições de segurança do que outros colaboradores, as viagens frequentes – contando com dispositivos móveis e Wi-Fi público – e as pessoas que os cercam, que também costumam ser privilegiadas no que diz respeito ao acesso à informação.

Em outras palavras, um executivo tem mais vetores de ataque do que o resto da organização.

Ao mesmo tempo, as ameaças cibernéticas estão entre os maiores riscos para as empresas atualmente:

- A receita pode cair depois de uma violação de dados, caso clientes e colaboradores deixem de confiar na organização;

- Uma invasão de rede pode custar a vantagem competitiva da marca se houver roubo de propriedade intelectual.

Sem um programa sólido de cibersegurança, pode ser apenas uma questão de tempo até que uma brecha empurre um negócio na direção do abismo.

O C-level tem vulnerabilidades diferentes em relação aos outros funcionários. E o treinamento e a preparação em segurança da informação devem refletir essas particularidades.

Aqui, vamos citar alguns elementos-chave na conduta, que pode ser pouco cuidadosa em alguns momentos, e no controle de exposições que devem ser considerados entre os C-level quando o assunto é cibersegurança:

"EU NUNCA SEREI UM ALVO"

Cibercriminosos, normalmente, não estão focados em apenas um executivo, mas em encontrar quem está mais vulnerável. A postura de excesso de confiança, reforçada pela crença do "nunca vai acontecer comigo", costuma facilitar os ataques desses criminosos.

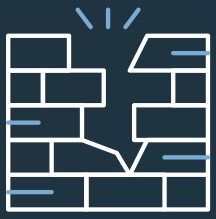
"Relatório de Investigações de Violação de Dados 2019" da Verizon

ESTRADA PARA O FUTURO

ANTIVÍRUS NÃO ASSEGURA 100% DA PROTEÇÃO

Antivírus certamente ajudam, mas, quando falamos de segurança cibernética, não há balas de prata. Proteção é uma abordagem complexa, feita em camadas, que envolve processos, tecnologia e pessoas especializadas.

AVALIAÇÕES DE VULNERABILIDADE EXECUTIVA



Quantificar a vulnerabilidade de risco cibernético dos executivos em toda a rede, incluindo suas famílias, é um bom jeito de começar. As avaliações devem cobrir não apenas o potencial de risco corporativo, mas também riscos individuais e familiares. Também é importante incluir um monitoramento na deep e dark web, para descobrir se dados de executivos já estão expostos.

CONTAS E DISPOSITIVOS PESSOAIS PROTEGIDOS

As contas privadas podem ser um ponto de entrada para o ambiente corporativo, seja através de reutilização de senha ou de logins em plataformas da empresa por meio de dispositivos pessoais.

Assim, um plano de segurança pode limitar quais dados corporativos os dispositivos podem armazenar ou acessar, levando em consideração quais contas podem ser comprometidas e exploradas a partir desses dispositivos.

O executivo também deve usar um IP dedicado em casa que esteja isolado do resto da rede doméstica. Que tipo de dados ele armazena ou tem acesso de casa precisa ser limitado, bloqueado ou fortalecido com criptografia.

ESTRADA PARA O FUTURO

NÃO SUPONHA QUE O SITE DO BANCO É 100% SEGURO

Os bancos com apps costumam aprimorar constantemente suas defesas. Mas, não existe nada que seja 100% seguro na web. Escrever a URL do site do banco com pressa pode levar a uma página falsa (criada por cibercriminosos para imitar endereços verdadeiros), em que o cliente tenha dados ou dinheiro roubados.

REDES WI-FI PÚBLICAS NÃO SÃO PARA COMPRAS E OPERAÇÕES BANCÁRIAS

Conexões públicas de Wi-Fi podem ser usadas por golpistas para enganar os usuários. Nesse ambiente, desconfie de links e use uma rede virtual privada (VPN) para criptografar dados importantes. Se estiver em um dispositivo móvel, use a rede da operadora para fazer transações importantes.

POLÍTICAS E PROCEDIMENTOS DE MÍDIA SOCIAL

Páginas como LinkedIn, Twitter, Facebook e Instagram, podem expor informações suficientes para um ataque de engenharia social, para rastreamento de locais físicos e para que o hacker entenda as fraquezas no sistema de TI corporativo.

Assim, é importante que executivos:

Desenvolvam diretrizes claras e fáceis de seguir sobre o que é aceitável compartilhar e o que pode colocar a organização em risco;

Mantenham contas pessoais privadas (quando são fechadas para o público em geral);

Tenham perfis públicos para evitar que um criminoso se aproprie de sua identidade nas mídias sociais.

ESTRADA PARA O FUTURO

AUTENTICAÇÃO DE DOIS FATORES E GERENCIADORES DE SENHAS

Executivos devem usar autenticação de dois fatores em contas pessoais, como Gmail ou Dropbox, bem como em contas corporativas. Da mesma forma, aplicativos de gerenciador de senhas para logins pessoais e profissionais. Isso porque muitas violações de dados ocorrem porque invasores ganham acesso a senhas que as pessoas reutilizam em várias contas.

VERIFICAÇÃO DE SOLICITAÇÕES

Os cibercriminosos usam informações públicas de executivos para se passarem por eles. Enviam a um funcionário do setor financeiro, por exemplo, um e-mail que parece ser desse executivo e pedem que a vítima transfira dinheiro da empresa para uma conta fraudulenta.

Portanto, o plano de segurança da organização deve ter processos para verificar se solicitações assim são legítimas. O objetivo não é sobrecarregar as pessoas com mais camadas de segurança, mas fazê-las tomar medidas extras quando forem realmente necessárias.

A CONFIABILIDADE DE SITES DEVE SER QUESTIONADA

Quem não questiona a legitimidade de páginas pode ser vítima de cibercriminosos. Isso porque navegar na Internet exige cuidado. Lembre-se de não clicar em anúncios incomuns e links recebidos por e-mail, ou mensagem de texto de desconhecidos.

CONHEÇA TODOS OS CONTATOS DIGITAIS

Aceitar solicitações de amizade de quem não conhece pode facilitar a entrada de malware ou de ladrões de identidade em seu ambiente.

ESTRADA PARA O FUTURO

CUIDADO PARA NÃO TRATAR COM INGENUIDADE DADOS IMPORTANTES

Divulgar informações importantes à rede de contatos estendida pode ser perigoso. Dados pessoais, como nome, a escola onde estudou ou a história da família, podem servir para responder às perguntas de segurança de senhas. Ajuste os controles de privacidade das redes sociais para limitar quem pode ver essas informações.

NÃO USE UMA ÚNICA SENHA PARA DIFERENTES SERVIÇOS

Se essa combinação for exposta, criminosos podem usá-la para ter acesso a diversas contas em plataformas diferentes. É mais seguro optar por várias senhas. Crie códigos fortes para evitar que sejam obtidos facilmente.

DESBLOQUEAR DISPOSITIVOS MÓVEIS À FORÇA NÃO É O IDEAL

O desbloqueio por jailbreak (ou à força) ajudam a habilitar produtos e recursos de forma extraoficial. Mas essa atividade também remove proteções e deixa o equipamento vulnerável a malwares. Para manter a segurança, evite esse método, bem como o acesso a sites de download duvidosos relacionados ao assunto e os demais perigos online que vêm com eles.

ESTRADA PARA O FUTURO

TOME ALGUNS CUIDADOS NO USO DO PIX E OUTROS APLICATIVOS DE TRANSFERÊNCIA DE DINHEIRO NO CELULAR

Estabeleça no aplicativo ou site do banco um limite diário para transações via Pix. Isso já evita que criminosos consigam retirar todo o seu dinheiro em apenas uma única transferência. Além disso, nunca realize transações fora dos canais oficiais do seu banco ou instituição. Tenha certeza que está no site ou aplicativo oficial. Os golpistas criam links e páginas muito similares às verdadeiras, mas analisando com calma é possível notar a diferença nos detalhes do endereço ou em algum erro ortográfico. Clicando no cadeado que fica na barra de endereço do navegador também é possível verificar se está navegando em um site seguro.

Não faça transações quando estiver conectado a redes de Wi-Fi públicas. Locais de acesso coletivo, como parques, bares ou shoppings, podem conter vírus e malwares que podem roubar dados para vender no mercado ilegal.

As chaves Pix cadastradas são outro ponto que precisam de cuidado ao serem divulgadas. Prefira passar chaves aleatórias. O CPF, passe somente para pessoas próximas e de confiança ou empresas com as quais você já se relaciona.

ESTRADA PARA O FUTURO

DEIXE O ACESSO A BANCOS E CONTAS DE CORRETORAS DE VALORES MAIS SEGURO

- **Bloqueie o IMEI**

O IMEI é como se fosse o número da “carteira de identidade” do aparelho. Ao bloqueá-lo, o usuário impede que um chip instalado naquele aparelho tenha uma linha de telefone ou internet daquela operadora que funcione ali.

- **Formatar o aparelho à distância**

Uma segunda opção para impedir que os criminosos tenham acesso aos dados financeiros do seu celular após um roubo ou furto é formatar o aparelho à distância. É o chamado ‘wipe remoto’ e o comando pode ser feito por meio do site do iCloud, sistema de armazenamento dos usuários de aparelhos Apple, ou por meio de softwares de antivírus no caso de aparelhos Android.

- **Senha no chip**

Uma outra dica muito importante é colocar uma senha no seu chip, que é diferente daquela senha que você usa para desbloquear o seu aparelho. Isso faz com que os criminosos não consigam acessar o seu chip de outro aparelho. Esse passo é importante porque muitos bancos usam SMS e ligações como mecanismos de recuperação de senha. Portanto, se aquele criminoso usar seu chip em outro aparelho, ele pode conseguir acesso às suas contas bancárias usando o recurso do “Esqueci minha senha”.

- **Não deixe cartão de crédito salvo no aparelho**

Precisar digitar o “código de segurança” do cartão não é o suficiente para que um criminoso não consiga usá-lo, caso o celular seja levado. O ideal é que, sim, você preencha o número do cartão de crédito a cada compra que você for fazer on-line. Considere usar um cartão virtual para cada compra feita.

E para finalizar, separamos 4 mitos que podem atrapalhar uma postura cibernética madura:

ESTRADA PARA O FUTURO

"NUNCA SOFRI UM ATAQUE CIBERNÉTICO, ENTÃO DEVO TER UMA POSTURA DE SEGURANÇA FORTE O SUFICIENTE"

1

As ameaças cibernéticas estão crescendo continuamente em sofisticação e complexidade, e precisamos nos esforçar continuamente para mantermos a proteção, tanto em tecnologias e processos, quanto em cultura e mentalidade. O objetivo não é alcançar a segurança perfeita, mas ter uma postura estratégica de segurança que o ajude a reagir rapidamente a um incidente e atenuar as consequências antes que cause danos irreversíveis.

"A SEGURANÇA É DE RESPONSABILIDADE DO DEPARTAMENTO DE TI"

2

Claro, a TI tem uma grande responsabilidade para gerenciar a segurança cibernética de uma organização. Mas, não deve ser o único responsável pela segurança. Como uma violação de segurança pode ter efeitos potenciais e duradouros em todo o negócio, a preparação real para a segurança cibernética é responsabilidade de todos. Principalmente dos executivos, que são alvos constantes de ataques.

"OS CIBERCRIMINOSOS NÃO TÊM COMO ALVO PEQUENAS E MÉDIAS EMPRESAS"

3

Pequenas e médias empresas muitas vezes pensam que são imunes a ataques cibernéticos e violações de dados. De acordo com um recente Relatório de Investigações de Violação de Dados da Verizon, 58% das vítimas de ataques cibernéticos são pequenas empresas. Elas nem sempre têm software de segurança avançado e equipes de segurança qualificadas, o que as tornam um alvo mais fácil para os cibercriminosos.

"SABEREI IMEDIATAMENTE SE ALGUM DE MEUS DISPOSITIVOS FOR INVADIDO"

4

Na era digital, é possível que leve meses ou até anos para uma pessoa perceber que sua segurança cibernética foi comprometida, e seu computador foi infectado. Porque as cepas modernas de malware são ainda mais furtivas e difíceis de detectar.

ESTRADA PARA O FUTURO

ACESSE

ISH.COM.BR