

GUIA DO NÍVEL CISO: PROTEGER OS SEUS CLIENTES

ADMINISTRAR CONTAS

- Peça aos clientes que utilizem ID de utilizador e palavras-passe fortes para iniciar sessão nos seus serviços. Aconselhe-os a não utilizar a mesma palavra-passe como o fazem para outras contas.
- Utilize a verificação instantânea, verificação em tempo real, verificação de "trial deposits", verificação da identidade e/ou perguntas pessoais para validar clientes reais e reduzir a oportunidade de fraude.
- Offer, ideally require, two-factor authentication for customers to log into your services.
- Verifique regularmente as contas do utilizador para sinais de fraude.

PROTEGER DADOS

- Considere quais os dados de clientes que a sua organização deve recolher para prestar os seus serviços e seja cauteloso na recolha de quaisquer dados de clientes que possam ir além dessa finalidade.
- Definir e distribuir políticas de retenção de dados. Elimine os dados do cliente quando já não forem necessários.
- Encripte os dados do cliente em trânsito e em repouso.
- Implemente políticas de segurança de dados para esclarecer quais os métodos de transferência de dados aprovados versus restritos e para especificar o que é aceitável para todos os funcionários ao lidar com dados de clientes. Certifique-se de que estas políticas são documentadas, comunicadas, aplicadas a todos os funcionários e revistas e atualizadas periodicamente.

PROTEGER APLICAÇÕES WEB PÚBLICAS

- Implemente HTTPS na(s) aplicação(ões) Web direcionadas para o público da sua organização e redirecione todo o tráfego HTTP para HTTPS.
- Utilize uma política de segurança de conteúdo no(s) seu(s) website(s) para evitar ataques de scripting entre sites, clickjacking e outra injeção de códigos.
- Permita a fixação de chaves públicas no(s) seu(s) website(s) para impedir ataques de intrusos.
- Ensure that your public-facing web application(s) never use cookies to store highly sensitive or critical customer information (such as passwords), follow conservative expiration dates for cookies (sooner rather than later), and consider encrypting the information stored in the cookies you use.
- Considere contratar um serviço de teste de invasão para avaliar a segurança da sua aplicação de rede pública, pelo menos, uma vez por ano.

Aconselhamento individual para clientes e funcionários para proteger dados financeiros

Aconselhe os seus funcionários e os seus clientes a seguir as orientações de cibersegurança abaixo no seu comportamento pessoal para aumentar a sua preparação e proteger os seus dados financeiros contra ameaças cibernéticas.

1. Implemente práticas básicas de higiene cibernética nos seus dispositivos.

- Utilize palavras-passe fortes em todos os dispositivos pessoais e profissionais e considere utilizar um gestor de palavras-passe.
- Mantenha os sistemas operativos e outros softwares e aplicações atualizados nos seus computadores e dispositivos móveis.
- **Instale** software antivírus, anti-malware e anti-ransomware que previne, deteta e remove programas maliciosos.
- Utilize um programa de firewall para impedir o acesso não autorizado ao seu computador.
- Utilize apenas produtos de segurança de empresas conceituadas. Leia comentários de publicações de computadores e consumidores e considere consultar o fabricante do seu computador ou sistema operativo.

2. Tenha cuidado com informações sensíveis.

- Não envie palavras-passe de contas bancárias ou outros dados de contas financeiras sensíveis por e-mail não encriptado.
- Seja inteligente sobre onde e como se estabelece a ligação à Internet para comunicações bancárias ou outras comunicações que envolvam informações pessoais sensíveis. As redes e computadores Wi-Fi públicos em locais como bibliotecas ou centros comerciais de hotéis podem ser arriscados.

3. Resistir ao phishing.

- Não abra imediatamente anexos de e-mail ou clique em ligações de e-mails não solicitados ou suspeitos. Pare. Pense. Clique.
- Suspeite se alguém o contactar inesperadamente online ou por telefone e pedir a sua informação pessoal. Mesmo quando comunica com endereços conhecidos, minimize a partilha de informações pessoais por e-mail.
- Lembre-se de que nenhuma instituição financeira irá enviar-lhe um e-mail ou contactá-lo e solicitar informações confidenciais que já tenha sobre si.
- Assuma que um pedido de informações de um banco onde nunca abriu uma conta é um esquema fraudulento.
- **Verifique** a validade de um e-mail de aspeto suspeito ou uma caixa pop-up antes de fornecer informações pessoais. Preste muita atenção ao endereço de e-mail.

FORMAR FUNCIONÁRIOS

- Ensine a responsabilidade e as estratégias dos seus funcionários para minimizar o erro humano que possa expor os dados dos clientes. Isto significa aconselhá-los a:
 - Minimizar o seu acesso e transmissão de dados de clientes apenas para o que é necessário para desempenhar as suas funções profissionais,
 - Manter fortes práticas de segurança em todos os dispositivos e contas que lidam com os dados do cliente utilizando palavras-passe fortes, permitindo a autenticação de dois fatores, mantendo o software atualizado e não clicando em ligações suspeitas, e
 - Comunicar quaisquer potenciais incidentes de segurança internos ou externos, ameaças ou manuseamento incorreto de dados ao pessoal técnico da sua organização e/ou a direção superior.
- Certifique-se de que os seus funcionários compreendem e assinaram documentos para aderir às políticas de proteção de dados e segurança da sua organização, para que não os violem, para que sejam fluentes ao lidar com os clientes e que não comuniquem com os clientes de forma desprotegida.

NOTIFICAR CLIENTES

- Compreender o ambiente regulamentar da sua organização no que diz respeito ao tratamento de violações de dados dos clientes para garantir que está preparado para cumprir quando ocorrem incidentes.
- Quando a sua organização toma conhecimento de um incidente de acesso não autorizado a informações sensíveis do cliente, investigue para determinar de imediato a probabilidade de a informação ter sido ou ser usada indevidamente. Siga as melhores práticas de notificação e notifique o(s) cliente(s) afetado(s) assim que possível com:
 - Uma descrição geral do incidente e a informação que foi violada,
 - Um número de telefone para mais informações e assistência,
 - Um lembrete “para permanecer atento” nos próximos 12 a 24 meses,
 - Uma recomendação para que os incidentes de suspeita de roubo de identidade sejam comunicados imediatamente,
 - Uma descrição geral das medidas tomadas pela instituição financeira para proteger a informação de acesso ou utilização não autorizados,
 - Informações de contacto para agências de informação comercial, e
 - Qualquer outra informação que seja exigida pelos regulamentos com os quais a sua organização deve cumprir.

