Cibersegurança Bancária

Estratégias para Proteger Dados e Evitar Fraudes

Ulysses Viudes

Fraudes Bancárias no Brasil

- No primeiro semestre de 2024, foram registradas mais de 1 milhão de tentativas de fraude no país. Isso representa uma média de mais de 4.600 tentativas de golpes financeiros por hora, evidenciando a frequência e a agressividade dessas atividades criminosas.

- Pesquisa Datafolha divulga em agosto de 2024, mostra que fraudes digitais e roubos de celular no Brasil resultaram em um prejuízo de R$ 71,4 bilhões em 1 ano. O levantamento considerou os crimes digitais com máquinas de cartão, boletos falsos e golpes com Pix.

OS DADOS SÃO ALARMANTES, DESTACANDO A URGÊNCIA DE AÇÕES PREVENTIVAS E DE CONSCIENTIZAÇÃO.

10 Estratégias para Proteger Dados e Evitar Fraudes Bancárias

A luta contra os cibercrimes é um desafio contínuo, mas, com estratégias adequadas, é possível proteger melhor o setor bancário e a população brasileira.

Pensando nisso este material apresenta 10 medidas estratégicas para proteger dados e coibir fraudes no setor bancário.

1. Autenticação Multifator (MFA)

Exija duas ou mais formas de autenticação para acessar sistemas críticos, como uma senha combinada com um código enviado por SMS ou gerado por um aplicativo de segurança.

Exemplo: Google Authenticator ou Microsoft Authenticator para logins corporativos.

2. Evite Redes Wi-Fi Públicas para Transações

Wi-Fi público pode ser inseguro, facilitando o acesso de hackers a seus dados.

Exemplo: Ao acessar sua conta bancária, prefira usar sua conexão 4G/5G ou uma VPN para proteger sua navegação..

3. Adote Senhas Fortes e Únicas

Crie senhas complexas e evite repetir as mesmas em diferentes contas.

Exemplo: Em vez de usar “123456” como senha, opte por algo como “#C@ix@2025!”.

4. Não Clique em Links Suspeitos

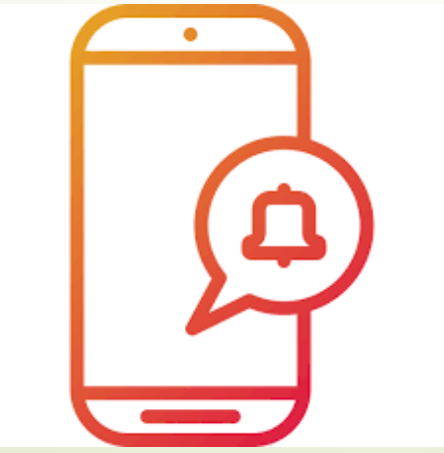
Golpes de phishing tentam roubar informações por meio de e-mails ou mensagens falsas.

Exemplo prático: Recebeu um SMS dizendo que sua conta será bloqueada? Antes de clicar no link, acesse o aplicativo do banco diretamente ou ligue para a central de atendimento.

5. Monitore Suas Transações Bancárias

Acompanhe frequentemente o extrato da conta para identificar movimentações não autorizadas.

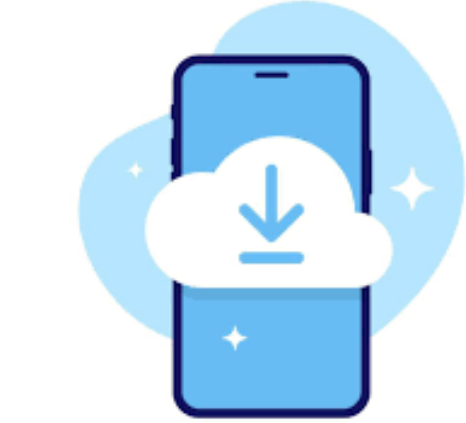
Exemplo: Ative notificações no aplicativo para receber alertas de cada movimentação em sua conta.



6. Atualize seus Dispositivos e Aplicativos

Manter sistemas operacionais e aplicativos atualizados é essencial para evitar vulnerabilidades.

Exemplo: Certifique-se de sempre instalar as atualizações oferecidas pelo seu banco, que geralmente incluem melhorias de segurança.



7. Desconfie de Ofertas Muito Boas

Golpes costumam envolver ofertas falsas para roubar dados.

Exemplo: Alguém oferece um "investimento garantido" via WhatsApp? Pesquise a empresa e procure informações oficiais antes de compartilhar qualquer dado ou dinheiro.

8. Ative o Bloqueio Automático do Dispositivo

Configure o bloqueio de tela no celular e no computador para impedir o acesso não autorizado.

Exemplo: Utilize senhas, biometria ou reconhecimento facial para desbloquear seus dispositivos.

9. Use Softwares de Segurança

Instale antivírus e configure firewalls para proteger seu computador e smartphone contra malwares.

Exemplo: Configure seu antivírus para verificar automaticamente qualquer arquivo baixado ou site acessado.

10. Eduque-se e Compartilhe Informações

Aprenda sobre os principais tipos de fraudes e compartilhe dicas com amigos e familiares.

Exemplo: Se você conhece alguém que caiu no golpe do Pix, compartilhe como identificar mensagens falsas para que outros não sejam vítimas.

Proteja o Que é Seu, Sua Segurança Bancária esta em Suas Mãos

Proteger os dados bancários é uma prioridade tanto para empresas quanto para os consumidores.

As Medidas apresentadas neste ebook tem o objetivo de orientar e conscientizar os usuário do sistema financeiro e bancário a proteger-se dos ataques cibernéticos.

Adotar essas e outras estratégias no dia a dia é essencial para proteger seus dados e garantir segurança financeira..

Agradecimentos

Este ebook é um exercício de estudo e aprendizado do curso de IA Generativa com Microsoft Copilot da DIO.

Neste material foram utilizados ChatGPT para o desenvolvimento do conteúdo, o Canvas para geração de algumas imagens e o Power Point para diagramação do material.

Agradeço ao Prof. Felipe Aguiar e a equipe da DIO.

https://web.dio.me/

E-book