Segurança em Foco

CPSI - Comissão Permanente de Segurança da Informação
SSI - Seção de Suporte e Segurança da Informação
ASCOM - Assessoria de Comunicação Social e Cerimonial

PHISHING

Edição nº10
Abril/2021

Phishing **é um dos golpes mais comuns na internet. Essa prática, como o nome sugere ("*phishing*" em inglês corresponde a "pescaria"), tem o objetivo de "pescar" informações e dados pessoais importantes através de mensagens falsas. Com isso, os criminosos podem conseguir informações tais como nome completo dos usuários, documentos de identificação, como identidade, CPF, contas bancárias, cartões de crédito, senhas e códigos de segurança entre outros. A diferença entre um golpe clássico e um phishing é o fato desse último induzir a vítima ao erro para que, voluntariamente, faça uma ação ou forneça informações.**

Os principais tipos de *phishing* são:

- **Blind Phishing: ocorre via disparo de e-mails em massa. Os criminosos contam com a ingenuidade e desconhecimento de parte dos destinatários. É comum, por exemplo, o e-mail ter algum link ou anexo tendencioso para que o receptor baixe um vírus em seu computador.**
- **Smishing: realizado por meio de disparos de SMS para celulares. Em geral, são mensagens que induzem a vítima a tomar decisões imediatas, como dizer que ela está endividada ou ganhou um sorteio inesperado.**
- **Scam: são tentativas dos criminosos de conseguir informações de vítimas por meio de links ou arquivos contaminados. Nesse tipo de Phishing, o contato pode ser feito por telefone, e-mail, mensagem de texto ou pelas redes sociais, por exemplo.**
- **Clone Phishing: esse golpe clona um site original para atrair os usuários e induzi-los a se comportarem como se estivessem em um ambiente seguro.**
- **Spear Phishing: é quando o ataque é direcionada uma pessoa ou grupo de vítimas em específico. Por isso, ele tem como objetivo acessar um banco de dados específico para obter informações sigilosas, arquivos confidenciais ou financeiros.**
- **Vishing: esse golpe utiliza mecanismos de voz para aplicar golpes na internet. Em geral, a chamada de voz cria uma sensação de urgência para que o usuário tome medidas e forneça informações rapidamente.**
- **Pharming: neste tipo de golpe, o tráfego de um site legítimo é manipulado para direcionar usuários para sites falsos e que podem instalar softwares maliciosos nos computadores dos visitantes. Além disso, ele é capaz de coletar dados pessoais, tais como senhas ou informações financeiras.**

Diante destas ameaças, seguem **7 dicas de como se proteger:**

1. **Antes de tudo, desconfie: desconfie de toda comunicação não desejada que você recebe. Desconfie, principalmente, caso receba uma mensagem de uma empresa sem ter realizado nenhuma ação recente na sua conta/plataforma. Em caso de dúvidas, entre em contato com a empresa pelos canais oficiais de atendimento.**
2. **Verifique os links antes de clicar: cuidado com links que você recebe em um e-mail, por exemplo. Mesmo que o conteúdo do e-mail fraudulento seja idêntico ao original, antes de clicar no link, pause o mouse sobre o link e confira se o domínio, que aparece no inferior esquerdo da tela, para o qual você seria direcionado é confiável.**
3. **Se atente a pequenos detalhes: é comum recebermos, em nossas redes sociais, anúncios de produtos de diversas lojas virtuais e e-commerces. E, em alguns desses casos, podem ser páginas falsas imitando quase que perfeitamente as páginas de produtos da marca. Por isso, antes de fechar uma compra ou inserir qualquer dado pessoal, veja se endereço de URL está correto, se valores são diferentes dos apresentados no site oficial e o que mais for útil para te ajudar a ter certeza de que está no site correto.**
4. **Instale antivírus em seus dispositivos: o antivírus é uma ótima ferramenta contra Phishing e outras táticas criminosas, especialmente porque ele costuma alertar contra conteúdos suspeitos. Por isso, busque um antivírus de qualidade, mesmo em versão gratuita.**
5. **Faça verificação em duas etapas: esse é um processo que envolve duas formas de acesso, uma seguida da outra, para checar se o usuário em questão é, de fato, a pessoa autorizada. Aplicativos como o Whatsapp já possuem essa função.**
6. **Use plugins no navegador anti-phishing: a dica é instalar plugins específicos nos navegadores para impedir o Phishing. Assim, cada vez que você acessar um site, a ferramenta faz a verificação automática de registros ou indícios desse portal nas listas de endereços banidos.**
7. **Identifique a autenticidade das cobranças recebidas: Fique atento aos dados apresentados nos boletos e em outras modalidades de cobrança. Certifique-se sobre a procedência da cobrança, busque por erros ortográficos ou informações falsas. Verifique, também, os números apresentados no código de barras do boleto.**

Fique ligado: no próximo mês, falaremos sobre Certificado Digital!

Tribunal Regional Eleitoral - RN