

Cuidado com Golpes de Phishing



As 5 principais formas que os fraudadores usam para roubar suas informações

Os cibercriminosos contam com o fato de estarmos distraídos e baixarmos a guarda. Se isso acontecer, eles podem nos enganar para que entreguemos nossas informações pessoais ou financeiras usando uma de suas táticas favoritas – o phishing.

Você pode estar familiarizado com o phishing por e-mail, mas esse não é o único tipo de golpe que pode acontecer. Criminosos também usam ligações telefônicas, mensagens de texto, sites e redes sociais para aplicar golpes de phishing.

Abaixo estão algumas formas comuns de phishing que você pode encontrar e os sinais de alerta aos quais deve prestar atenção.

Phishing por ligação telefônica

Sinais de alerta

- 1 Uma ligação do “seu banco” ou “instituição financeira”, geralmente de alguém que diz trabalhar no “Departamento de Segurança e Fraudes”.
- 2 Informam que seu cartão foi sinalizado por transações suspeitas e que você precisa **provar que está com o cartão** em sua posse.
- 3 Pedem que você forneça o **código de segurança de três dígitos** no verso do cartão, um código de verificação enviado por SMS naquele momento ou seu PIN.



Phishing por e-mail



Sinais de alerta

- ❌ Erros de ortografia e gramática no assunto ou no corpo do e-mail.
- ❌ O e-mail não se dirige a você pelo nome.
- ❌ Prazo. Às vezes, golpistas incluem um prazo e ameaçam suspender a conta para criar urgência e reduzir sua cautela.
- ❌ Ausência de informações de contato. Se algo parecer suspeito, entre em contato diretamente com sua instituição financeira usando o número no verso do seu cartão.
- ❌ O endereço de e-mail não corresponde à organização (por exemplo, irs.net ou amazon.ml).
- ❌ Links suspeitos. Evite clicar em links sempre que possível. Um único clique pode infectar seu computador com malware.

Phishing por mensagem de texto

Sinais de alerta

- 📄 Há um link em vez de um número de telefone para ligar.
- 📄 A mensagem pode não conter o nome do banco ou outras informações relevantes.
- 📄 A mensagem solicita que você faça login na sua conta bancária para verificar uma transação, informe seu PIN ou forneça o código CVV de 3 dígitos.



Phishing por site



Sinais de alerta

- 🔍 Algo parece ligeiramente errado no endereço do site ou na própria página. Procure palavras escritas incorretamente, substituições ou logotipos alterados.
- 🔍 Um pop-up incomum no site solicitando que você informe os dados da sua conta.
- 🔍 Links em HTML que não correspondem ao destino real.

Phishing em redes sociais

Sinais de alerta

- 👍 Pedido de amizade de alguém que você não conhece.
- 👍 Publicação pedindo para clicar em um link que solicita informações pessoais.



Você já foi vítima de um golpe de phishing?

Para mais informações sobre phishing e outros golpes digitais, visite a National Cyber Security Alliance em: <https://staysafeonline.org/>