Que o brasileiro está cada vez mais conectado à internet ninguém duvida. A pandemia da covid-19 acelerou a transformação digital já em curso, mas que vinha ocorrendo numa velocidade mais lenta. Na ocasião, o próprio Infraprev adotou alguns novos procedimentos internos, visando facilitar e modernizar o atendimento aos participantes.

Que o brasileiro está cada vez mais conectado à internet ninguém duvida. A pandemia da covid-19 acelerou a transformação digital já em curso, mas que vinha ocorrendo numa velocidade mais lenta. Na ocasião, o próprio Infraprev adotou alguns novos procedimentos internos, visando facilitar e modernizar o atendimento aos participantes.

A nova realidade on-line, no entanto, é uma via de mão dupla. Se por um lado traz facilidades ao usuário, no sentido oposto aumenta a exposição aos riscos de golpes cibernéticos, que estão se tornando cada vez mais comuns e inovadores. Alguns dos principais motivos para o aumento de golpes na internet, segundo especialistas, é a baixa exposição dos criminosos combinada com a facilidade de acessar e fraudar dados sensíveis dos usuários, além de ser mais fácil se fazer parecer com algum ente de confiança da vítima, persuadindo-a com maior facilidade e rapidez.

Outro aspecto importante é que as transações financeiras cada vez mais ocorrem por meios digitais, como o PIX e cartões de débito e crédito. Isso diminui a circulação de dinheiro na praça, levando os criminosos a migrarem para outras modalidades de delito. A boa notícia é que o comportamento do usuário é fundamental para minimizar o risco de ser vítima de um crime cibernético.

Mas o que é um golpe?

Qualquer situação em que sejam apresentadas informações falsas para tirar vantagem de alguém. Alguns são mais fáceis de identificar, especialmente quando trazem anúncios com ofertas mirabolantes e comunicações com texto e identidade visual suspeitos. Outros são mais complexos e precisam de atenção, como os e-mails com boletos falsos em anexo, mensagens

em redes sociais ou aplicativos de conversa se passando por entes próximos, entre outros.

Segundo levantamento da empresa de soluções de cyber segurança Fortinet, com base nos dados do FortiGuard Labs, no ano passado aconteceram cerca de 360 bilhões de tentativas de ataques cibernéticos aos sistemas organizações na América Latina e Caribe. O Brasil foi o segundo país com mais registros de ataques, com 103,1 bilhões de tentativas, atrás apenas do México, com 187 bilhões de tentativas em 2022.

Os principais ataques incluem fraude por e-mail e pela Internet, roubo de informações pessoais, de dados financeiros ou de pagamento de cartão. No entanto, diariamente surgem novos golpes na praça, utilizando até mesmo a inteligência artificial, que está cada vez mais acessível e com recursos impressionantes.

Numa modalidade que vem se tornando mais frequente, criminosos acessam vídeos e publicações nas redes sociais para pegarem o áudio do telefone e, a partir daí, simular a voz de pessoas e realizarem transferências bancárias fraudulentas. Com os dados do usuário em mãos, o golpista entra em contato e se apresenta como uma instituição financeira, falando que a conta supostamente foi hackeada. Para inibir essas ações fraudulentas, as instituições financeiras têm alertado que não pedem senhas ou quaisquer informações sigilosas por e-mail ou telefone. Portanto, é bom ficar atento.

Conheça alguns tipos de golpe aplicados pela Internet:

Roubo de identidade

Ocorre quando alguém usa o nome de outra pessoa, criando sites e perfis de redes sociais com identidade falsa, por exemplo. Isso pode ser feito, entre outros motivos, para ganhar dinheiro com atividades ilícitas.

Fraude de antecipação de recursos

Quando alguém tenta convencer uma pessoa a fazer uma “antecipação” de valor, com a promessa de devolução do dinheiro e outras compensações no futuro. É o famoso golpe que promete depositar milhões na conta do usuário mediante o pagamento de uma taxa da operação bancária.

Phishing

Quando alguém convence uma pessoa a fornecer seus dados pessoais, que podem ser usados para golpes e atividades ilícitas. Uma das formas mais comuns de phishing são os e-mails falsos que trazem anexos infectados, como fotos e vídeos. Ao baixar o anexo, o usuário instala um programa “espião” que coleta informações pessoais.

Nesta categoria entram os e-mails que podem ser, por exemplo, de uma operadora de telefonia, cobrando débitos via boletos. Como não reconhece os valores, a pessoa fica em dúvida baixa o arquivo para entender melhor a cobrança. Ao clicar, o usuário libera os dados para os criminosos e se torna mais uma vítima.

Pharming

Ocorre quando alguém redireciona uma pessoa para um site falso, diferente daquele que ela pensa estar acessando. Isso acontece, por exemplo, quando o usuário recebe um e-mail supostamente enviado pelo seu banco ou em uma superoferta de uma loja famosa. Ao clicar no link para acessar o site, é levado a uma página que parece legítima, mas não é. Qualquer informação inserida nessa página é enviada para os responsáveis pelo golpe.

Existem orientações para evitar golpes. Fique atento a partir de agora:

Dupla autenticação

A confirmação em duas etapas é uma forma de adicionar uma camada extra de segurança às

suas redes sociais. Nesse caso, se alguém tentar fazer login no seu perfil, além da senha, pode ser solicitada uma segunda confirmação de dados por e-mail ou SMS. A ideia é ter certeza de que é você mesmo quem está tentando acessar a conta pessoal. Alguns dispositivos como smartphones, podem adotar o uso do reconhecimento facial ou da impressão digital também.

Evite a exposição online

As informações compartilhadas em redes sociais podem ser usadas por criminosos que tentam aplicar golpes virtuais. Dados como nome completo ou CPF podem servir para o golpe do boleto falso. Uma boa dica para se proteger é deixar seus perfis de redes sociais privados, quando apenas as pessoas que você autoriza podem ver as informações compartilhadas.

Cuidado antes de fazer compras online

Ao ver algum anúncio de produto ou serviço, analise antes com cuidado. Converse com a pessoa que está vendendo, faça perguntas, questione sobre detalhes. Se for uma loja, garanta que o anúncio foi feito em perfis oficiais, veja se as condições do produto fazem sentido. Desconfie de condições vantajosas demais e de páginas com erros ortográficos na oferta. Caso não tenha certeza de que o remetente de um e-mail é confiável, não responda nem abra qualquer anexo.

Um dos indícios de perfil falso nas redes sociais é um número muito baixo de seguidores. Vale conferir, porque se a conta foi criada recentemente, provavelmente não terá muita gente seguindo. Hoje em dia, é muito comum golpistas usarem o nome de marcas conhecidas para aplicarem golpes.

Use dispositivos seguros

Não é recomendado acessar e a internet por computadores ou celulares de outras pessoas ou conectados a redes públicas de wi-fi. Uma dica para evitar que hackers possam capturar suas informações pessoais é usar dispositivos e conexões seguros. Evite redes de wi-fi abertas como em aeroportos, rodoviárias e shopping centers.

WhatsApp e redes sociais

Os golpes no WhatsApp são cada vez mais comuns, e é preciso ficar bem atento. Uma fraude comum é aparecer uma mensagem de um contato dizendo que trocou de número. De repente, a pessoa dá uma desculpa e diz que precisa de dinheiro rápido. Desconfie sempre. Antes de fazer qualquer transferência, ligue para a pessoa, converse com ela e garanta a autenticidade da mensagem.

Outra possibilidade é ter o WhatsApp clonado. Isso pode acontecer caso o usuário clique em um link desconhecido. Em alguns casos, esse link autoriza outra pessoa a ter acesso ao seu app de mensagens. É possível que esse golpe também seja usado para “sequestrar” outras redes, como Twitter, Instagram e Facebook.

O que fazer para se proteger?

- Ative a confirmação de duas etapas e tenha um e-mail para redefinir as senhas e códigos, caso você esqueça.
- Não compartilhe códigos de autenticação da conta com outras pessoas.
- Tenha uma senha para seu aparelho ser desbloqueado apenas por você.
- Desconfie de mensagens diferentes do que você está acostumado a trocar com seus contatos.
- Desconfie quando a foto de perfil do contato estiver vinculada a um número que você não tem na sua agenda.
- Antes de fazer qualquer transferência ou depósito, entre em contato com a pessoa, pelo número anterior, sem ser o que está vinculado à foto nova.

O que fazer se, por acaso, eu for vítima de um golpe pela Internet?

- Ao notar que caiu em um golpe pela Internet, mantenha a calma. Existem medidas que você pode tomar para minimizar os prejuízos.
- A primeira coisa é acionar a polícia. Procure uma delegacia e faça um Boletim de Ocorrência, para que a situação fique registrada.
- Em seguida, bloqueie cartões de crédito e débito, carteiras virtuais e demais serviços financeiros que você considera que podem estar expostos. Assim você evita, por exemplo, ter

seu cartão clonado.

- Informe às instituições financeiras, para que elas também fiquem atentas a movimentações estranhas em seu nome. E não se esqueça de trocar as senhas que podem ter vazado. Isso vale para senhas de e-mail, redes sociais, contas bancárias e de qualquer outro site ou serviço. Até mesmo senhas de Netflix ou Uber, por exemplo.
- Por fim, avise seus parentes e amigos. Suas informações podem ser usadas pelos responsáveis pelo golpe para entrar em contato com pessoas próximas a você, pedindo dinheiro. Se eles estiverem cientes, não correrão o risco de cair no golpe.

Fonte: Infraprev , em 17.10.2023.