O que é phishing e como se proteger de golpes na internet

Atualmente, em função das facilidades que o “mundo” virtual vem nos proporcionado, estamos utilizando-o cada vez mais, desde o pagamento de uma conta até a compra de um produto, isso sem contar, é claro, no quesito entretenimento, pelo qual diariamente acompanhamos diversas redes sociais como, por exemplo, Facebook e Instagram.

Contudo, simultaneamente, estamos muito mais vulneráveis às ameaças virtuais e crimes cibernéticos, onde criminosos se aproveitam do ambiente virtual para cometer infrações, preponderantemente, os casos de phishing.

Phishing é um tipo de crime cibernético em que um criminoso finge fazer parte de uma instituição legítima para convencer as vítimas a entregarem suas informações pessoais e confidenciais como, por exemplo, nome de usuário, número de cartões de crédito e senhas de banco. Os hackers costumam contatar seus alvos via e-mail, telefone ou mensagens de texto e geralmente se aproveitam de táticas de comunicação ou identidades visuais que remetem ao estilo de empresas conhecidas.

Por isso, tendo em vista que tal prática, infelizmente, é bastante comum em nosso cotidiano, é de extrema importância que saibamos quais são os tipos de phishing e como reconhecê-los a fim de possamos proteger nossos usuários e negócios desse perigo online.

O termo phishing foi eleito devido à semelhança com outra palavra do vocabulário inglês, fishing, a qual significa pescar. Ou seja, faz-se referência a prática de “pescar” os dados confidenciais dos usuários através de informações falsas, contudo, revestidas de suposta veracidade.

Portanto, assim como na pesca, o criminoso que pratica o phishing consegue informações sigilosas através de uma isca lançada aos usuários para então obter as ações que precisam para aplicar os golpes.

Nesse crime virtual pessoas comuns são contactadas através de e-mail, telefone ou mensagens de texto (SMS) por uma outra pessoa ou empresa. O contato se faz de maneira genuína, para atrair e induzir o contactado a fornecer informações sigilosas dados bancários, cartão de crédito, senhas e outras informações confidenciais.

Então, ao compartilhar estas informações, as pessoas têm sua conta e cartão violados, e podem ser vítimas de crimes de falsa identidade ou até mesmo perder dinheiro através de transações financeiras indesejadas.

Ademais, podem chegar até você falsos sítios eletrônicos e falsos pop-ups inseridos em sites desprotegidos, todos com uma abordagem atrativa.

Já os conteúdos podem ser dos mais variados como, por exemplo, em nome de bancos, governo, instituições financeiras (como PayPal) ou até mesmo correios, sempre solicitando uma ação ou informação, sendo a dinâmica mais usual consistente no pedido para que abra determinado link ou arquivo, ou, para que faça ligação ou instale/atualize um software específico.

Nesse sentido, vale destacar os tipos de phishing, quais sejam:

- **Scam** que são tentativas dos criminosos de induzi-lo a fornecer informações pessoais, como números de contas bancárias, senhas e números de cartão de crédito, através da abertura de links ou arquivos contaminados;
- **Blind Phishing** o qual é disparado via e-mail em massa e sem muitas estratégias contando apenas com a “sorte” de que algum usuário caia na armadilha;
- **Spear Phishing** que é quando o ataque é contra um grupo específico, então, pode ser contra funcionários do governo, clientes de uma empresa específica ou até mesmo uma pessoa específica;
- **Clone Phishing** o qual clona um site original para atrair os usuários e, geralmente, ao acessar o site falso, a pessoa tem que inserir informações cadastrais em um formulário malicioso que transmitirá as informações para os criminosos;
- **Whaling** a nomenclatura vem da palavra whale (baleia, em inglês) e quer dizer caçando baleias, isto é, este crime está ligado ao “tamanho do peixe a ser pescado”, eis que mira executivos de alto nível ou personalidades de relevância;
- **Vishing** em que a letra “p” foi trocada pelo “v” porque o vishing utiliza mecanismos de voz para aplicar golpes e, assim, podem vir acompanhados de SMS que dizem que o seu cartão foi bloqueado e você precisa ligar para um determinado número para pedir a liberação, ou também pode ser uma ligação direta para sua casa ou seu celular;
- **Pharming** que é quando acontece o envenenamento do DNS (o sistema que traduz os números dos IP’s em nomes de domínio) e atinge os usuários em uma larga escala e, por fim;

- **Smishing** que é o nome para phishing realizado através de SMS, isto é, são mensagens que geralmente constrangem o usuário como dívidas ou que impulsionam a tomar decisões imediatas pela emoção como sorteio, prêmios ou um valor alto a receber.

Vale lembrar que os ataques também estão presentes nas redes sociais. Propagandas e campanhas imperdíveis (que não existem), suporte incrível (que não é na verdade um suporte) ou também aquela mensagem que nos deixa curiosos: “alguém te marcou em uma foto, clique aqui para conferir”, enfim.

Portanto, como já dizia o ditado “quando a esmola é demais, o santo desconfia”. Assim sendo, se você receber ofertas muito lucrativas, declarações de ganhadores de prêmios, frases de efeito como “seu serviço será suspenso” ou “sua conta foi bloqueada, clique aqui para verificar”, e-mails ou mensagens acompanhadas de links externos para você clicar, desconfie, pois, muito provavelmente são apenas iscas para atrair o seu clique em links maliciosos que vão roubar os seus dados.

Dessarte, diante de tantas maneiras de ser atacado virtualmente, as formas de se proteger dos ataques de phishing englobam além de se manter informado e atento a todos os detalhes aqui expostos, algumas ações pontuais como, por exemplo, instalar antivírus, bem como um software firewall. Outrossim, avaliar as intenções e informações de e-mails, mensagens e ligações recebidas. Assim, se logrará êxito em evitar “cair” nessas armadilhas virtuais em que todos nós estamos expostos diariamente.

Fernanda do Couto Ferreira
Advogada do escritório MZ Advocacia
fernanda@mzadvocacia.com.br