Como reconhecer tentativas de phishing em aplicativos de mensagens populares

Aluno: Lucas Mariano
Sistemas de Informação, Estácio

Nesse conteúdo falaremos sobre como reconhecer tentativas de phishing. Mas afinal, o que é phishing?

Phishing é um crime cibernético que visa roubar informações confidenciais. Os hackers se disfarçam de grandes corporações ou de entidades confiáveis para induzir você a fornecer voluntariamente informações como credenciais de login e números de cartões de crédito.

Geralmente é uma mensagem falsa elaborada para parecer legítima e normalmente solicita que você forneça informações pessoais confidenciais fazendo uso de vários artifícios. No entanto, se você não prestar bem atenção aos e-mails ou mensagens de texto, talvez não consiga ver a diferença entre uma mensagem normal e uma mensagem de phishing. Os hackers se esforçam muito para fazer com que as mensagens de phishing se pareçam a e-mails e mensagens de texto enviados por empresas confiáveis, por isso você precisa ter cuidado ao abrir essas mensagens e clicar nos links contidos nelas.

A seguir, acompanhe como identificar essa tentativa de ataque.

Como identificar o phishing?
Os hackers de phishing geralmente cometem erros simples que são fáceis de detectar quando você sabe como reconhecê-los. Verifique os seguintes sinais:

1. Está mal escrito
   - As mensagens de phishing contêm frequentemente erros gramaticais, ortográficos e outros erros flagrantes que as grandes corporações não cometeriam. Se vir vários erros gramaticais chamativos em um e-mail ou mensagem de texto que pede suas informações pessoais, você pode estar sendo alvo de uma fraude de phishing.

2. O logotipo/design não parece correto
   - Para melhorar as possibilidades de enganar você, os hackers de phishing costumam roubar os logotipos das empresas pelas quais se fazem passar. Em muitos casos, no entanto, eles não roubam logotipos corporativos corretamente. O logotipo em um e-mail ou mensagem de texto de phishing pode ter a proporção errada ou baixa resolução. Se você tiver que forçar a vista para ver o logotipo em uma mensagem, é provável que seja phishing.

3. O URL não corresponde
   - O URL é o link. O phishing sempre usa links nos quais se supõe que você deve clicar. Aqui estão algumas maneiras de verificar se um link enviado a você é legítimo:

A) Passe o mouse sobre o link no e-mail para exibir o URL. Muitas vezes, os URLs de phishing contêm erros de ortografia, o que é um sinal comum de phishing. Ao colocar o mouse sobre o link, você poderá ver uma visualização prévia do link. Se o URL parecer suspeito, não clique nele e exclua a mensagem.
B) Antes de excluí-la, você também pode clicar com o botão direito no link e copiar e colar o URL em um processador de texto. Isso permite examinar o link completamente em busca de erros gramaticais ou ortográficos, sem ser direcionado para a página da Web potencialmente mal-intencionada.
C) Verifique o URL de um link em dispositivos móveis mantendo-o pressionado. Se o URL não corresponder à entidade que supostamente enviou a mensagem, você provavelmente recebeu um e-mail de phishing.

Os e-mails de phishing funcionam apenas com as pessoas desatentas. Agora que você já sabe como identificar e-mails de phishing e o que fazer se suspeitar que hackers estão atacando você, é muito menos provável que caia nessas artimanhas.

Lembre-se de ter cuidado com as informações pessoais ao usar a Internet e seja cauteloso sempre que alguém solicitar detalhes confidenciais sobre sua identidade, dados financeiros ou informações de login.