GOLPE DO INSTAGRAM FINGE SER SUPORTE DA META PARA ROUBAR CONTAS; SAIBA COMO EVITAR

Criminosos estão usando um novo golpe no Instagram para tomar o controle de contas de usuários, segundo alerta da empresa de cibersegurança Norton. O esquema consiste em enviar mensagens diretas (DMs) se passando por perfis oficiais da Meta, com o objetivo de induzir a vítima a clicar em um link fraudulento que rouba suas credenciais de acesso, como login, senha e até o código de autenticação em duas etapas.

De posse da conta, os golpistas passam a praticar crimes como extorsão e fraudes usando o perfil invadido. Os alvos mais comuns são influenciadores digitais, criadores de conteúdo, pequenos negócios e políticos, cujas contas geralmente têm grande alcance e valor estratégico.

Como os criminosos agem?

As vítimas recebem uma DM alertando sobre uma suposta violação das regras da plataforma e a ameaça de que a conta será desativada. A mensagem vem acompanhada de um link externo, que leva a uma página falsa, mas visualmente semelhante ao site da Central de Ajuda da Meta. Ali, o usuário é induzido a clicar em "Solicitar Revisão", e para continuar, precisa fornecer dados como login, senha e até o código de autenticação em dois fatores.

A partir desse ponto, os fraudadores assumem a conta, bloqueiam o dono original e utilizam o perfil para aplicar golpes em seguidores ou extorquir a vítima em troca da devolução do acesso.

Como se proteger?

Sanchez-Rola recomenda seguir algumas boas práticas para evitar cair nesse tipo de armadilha:

- Nunca clique em links enviados por desconhecidos;
- Confirme se o perfil do remetente tem o selo de verificação oficial
- Desconfie de mensagens com tom urgente ou ameaçador;
- Ative a autenticação de dois fatores em todas as suas contas;
- Denuncie qualquer comportamento suspeito ao Instagram;
- Utilize soluções de segurança digital, especialmente em perfis corporativos;
- Oriente equipes e colaboradores sobre riscos, principalmente em dispositivos compartilhados.