

ESET alerta para golpe com contas clonadas no Instagram



Os golpes de engenharia social vigentes e o roubo de identidade para obter lucro monetário aumentaram nas redes sociais. A ESET, empresa líder em detecção proativa de ameaças, explica como funciona essa ameaça e compartilha dicas para que usuários evitem cair nesses golpes.

Para entender como os usuários lidam com essas fraudes, o pesquisador da ESET Jake Moore decidiu clonar sua própria conta, com um telefone reserva e tirando quatro capturas de tela de sua conta original para imitar as ações dos cibercriminosos. A única diferença em seu novo relato, além do número de seguidores, foi uma mudança na biografia em que incluiu um texto que dizia "NOVA CONTA APÓS PERDA DE ACESSO AO ORIGINAL".

Em seguida, passou a seguir 30 de seus amigos, 10 de contas privadas, com exigência de aceitação, e 20 de contas públicas.

"Eu esperava que alguém me contatasse por um meio de comunicação diferente e questionasse esse pedido, principalmente por conta do meu trabalho e a vergonha a que poderia ter sido submetido, embora também entendo que todos somos suscetíveis a comprometimentos de conta. Mas ninguém o fez. Na verdade, os números aumentaram", comentou Jake Moore.

Replicando as ações dos cibercriminosos, ele enviou uma mensagem aos seus seguidores, agradecendo-os por aceitarem o novo pedido e mencionando o incidente, lamentando também que tenham atacado suas contas bancárias e que ele não tivesse dinheiro até que o problema fosse resolvido. O interlocutor, acreditando estar falando com o responsável pela conta, acha a conversa mais confiável e oferece sua ajuda.

"O que eu achei mais desconcertante foi a rapidez com que tudo aconteceu e que fui capaz de enganar o alvo pretendido fazendo-o pensar que era genuíno, sem a necessidade de verificação adicional. Conseguí até mesmo fazer com que a própria pessoa me oferecesse ajuda, o que deu um toque especial. Muitas vezes, essa é uma técnica inteligente usada por engenheiros sociais profissionais que fazem um jogo psicológico para evitar pedir o dinheiro diretamente", acrescentou o investigador da ESET.

Neste sentido, a ESET traz algumas recomendações sobre como manter as contas nas redes sociais seguras:

- Na medida do possível, reduzir a quantidade de informações pessoais e fotos online. Ainda que

seja uma grande tarefa, é importante ensinar à próxima geração de usuários das redes sociais a importância de limitar a quantidade de informações que se publica antes de estar exposto para sempre. Esse golpe não funcionaria da mesma maneira em contas privadas, mesmo que existam contas privadas que aceitam pessoas que não conhecem.

- Verificar o conteúdo do que é publicado. Também se aplica a aceitar seguidores, tomar alguns minutos para decidir se está disposto a que esse usuário conheça mais detalhes sobre seu dia a dia. Por sua vez, ser completamente público está sujeito a perigos como este.
- Quando houver dinheiro envolvido, nunca aceitar nada nem fornecer informações confidenciais sem analisá-las cuidadosamente. É essencial solicitar a validação por outra forma de comunicação antes de enviar dinheiro a um novo beneficiário ou compartilhar informações de conta ou cartão de crédito.

"Esse golpe não se limita apenas ao Instagram, ele também foi visto no Facebook, Twitter e LinkedIn, portanto, fique de olho nas contas clonadas. Reporte essas contas e informe o verdadeiro dono das mesmas. Nós, da ESET, apostamos na educação como a primeira ferramenta de proteção. Conhecer os riscos a que estamos expostos permite-nos tomar medidas para prevenir ameaças: manter os nossos sistemas atualizados, ter uma [solução de segurança nos nossos dispositivos](#) e saber as novidades em termos de ataques ajudam a desfrutar da tecnologia com segurança", explica Luis Lubeck, especialista em segurança da informação da ESET América Latina.

Para te ajudar a ficar em casa

A ESET aderiu à campanha [#FiqueEmCasa](#), oferecendo proteção para dispositivos e conteúdos que ajudam os usuários a aproveitar os dias em casa e garantir a segurança dos pequenos enquanto se divertem online em meio à pandemia.

No site, os usuários podem ter acesso a: ESET INTERNET SECURITY grátis por 3 meses para proteger todos os dispositivos domésticos, Guia de Teletrabalho, com práticas para trabalhar em casa sem riscos, Academia ESET, para acessar cursos online que auxiliam a tirar mais proveito da tecnologia e o [DigiPais](#), para ler conselhos sobre como acompanhar e proteger crianças na web.

A ESET possui o portal [#quenãoaconteca](#), com informações úteis para evitar que situações cotidianas afetem a privacidade online.

Para saber mais sobre segurança da informação, entre no portal de notícias da ESET: <http://www.welivesecurity.com.br/>

Sobre a ESET

Desde 1987, a ESET® desenvolve soluções de segurança que ajudam mais de 100 milhões de usuários a aproveitar a tecnologia com segurança. Seu portfólio de soluções oferece às empresas e consumidores de todo o mundo um equilíbrio perfeito entre desempenho e proteção proativa. A empresa possui uma rede global de vendas que abrange 180 países e possui escritórios em Bratislava, San Diego, Cingapura, Buenos Aires, Cidade do México e São Paulo. Para mais informações, visite <http://www.eset.com/br> ou siga-nos no [LinkedIn](#), [Facebook](#) e [Twitter](#) .

Copyright © 1992 - 2020. Todos os direitos reservados. ESET e NOD32 são marcas registradas da ESET. Outros nomes e marcas são marcas registradas de suas respectivas empresas.

<https://www.territoriopress.com.br/noticia/1537/eset-alerta-para-golpe-com-contas-clonadas-no-instagram> em 18/12/2025 19:35