Necessidade de saber

Principais descobertas do *State of the Phish de 2023*

Os riscos crescentes de um local de trabalho híbrido e dos ataques cibernéticos cada vez mais avançados são bem compreendidos pelos CISOs. Mas a conscientização quanto à segurança e os comportamentos dos usuários finais melhoraram desde o ano passado? Infelizmente, a resposta curta é “não”.

Os ataques e as perdas financeiras decorrentes explodiram em 2022, enquanto o nível de conscientização dos usuários estagnou e algumas métricas de treinamento pioraram. Segue uma classificação de nossas principais descobertas.

44%

das pessoas pensam que um e-mail é seguro quando contém marcas familiares

300K-400K

tentativas de entrega de ataques voltados para telefones por dia, com um pico de 600 mil por dia em agosto de 2022

1/3

das pessoas executaram uma ação arriscada (como clicar em links ou fazer download de malware) diante de um ataque

76%

de aumento em perdas financeiras diretas associadas a phishing bem-sucedido

30 milhões

de mensagens maliciosas enviadas em 2022 envolveram produtos ou marcas da Microsoft

Mais de 1 em cada 10

ameaças foram bloqueadas como resultado de denúncias de usuários

APENAS **35%** das organizações realizam simulações de phishing

Nem mesmo conceitos básicos são compreendidos

64% das organizações infectadas por ransomware pagaram resgate

90% das organizações afetadas por ransomware tinham uma política de seguro cibernético

65% das organizações relataram pelo menos um incidente de perda de dados por elementos internos

APENAS **56%** das organizações com um programa de conscientização quanto à segurança treinam todos os seus funcionários

dos profissionais de segurança consideram a segurança uma prioridade em suas empresas

versus

dos funcionários afirmam que a segurança cibernética não é uma prioridade no trabalho

Para obter mais detalhes, dados e insights, faça o download do relatório *State of the Phish de 2023* da Proofpoint.

proofpoint.

0704-002-07-01