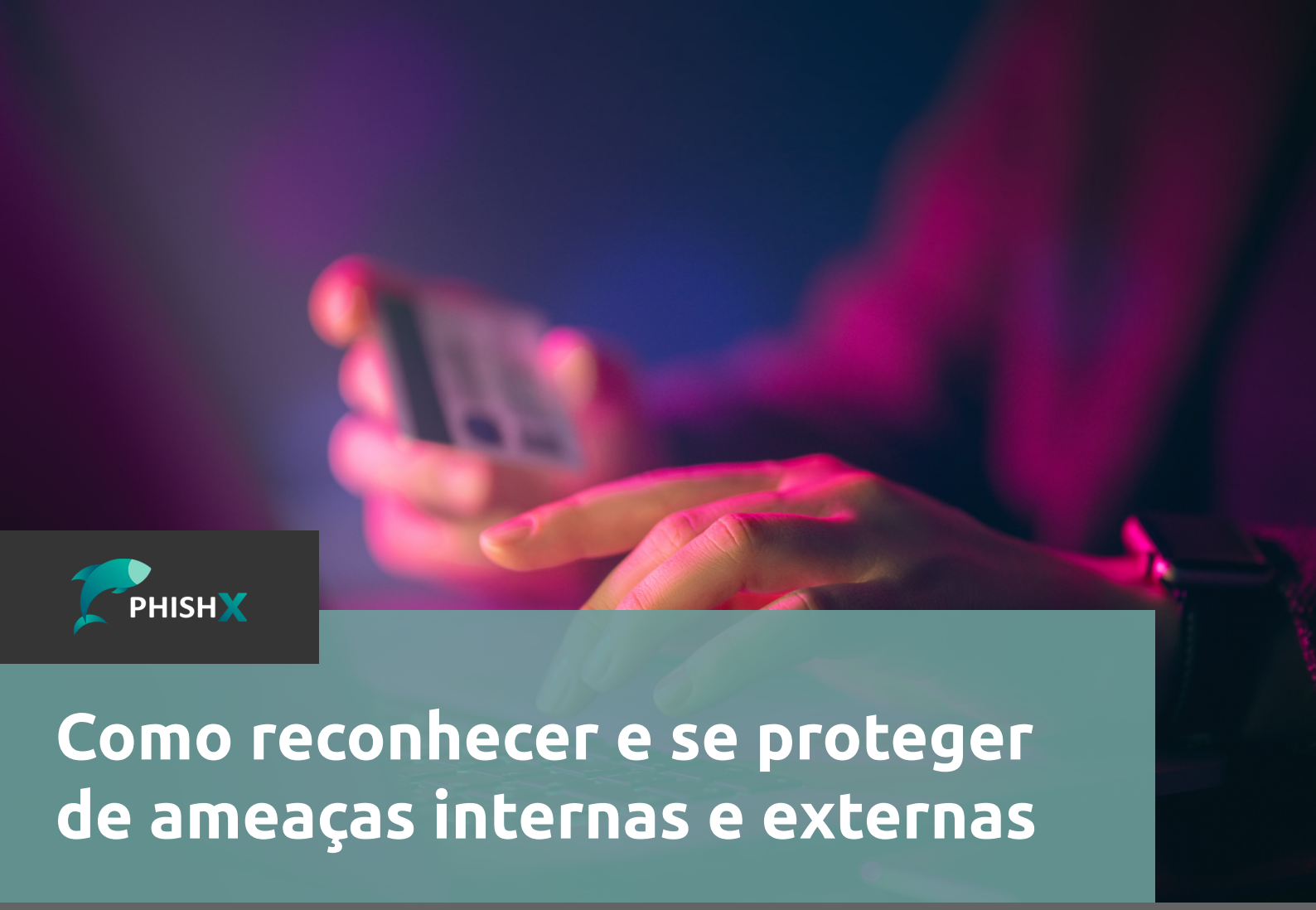

PHISHX

Como reconhecer e se proteger de ameaças internas e externas

O que são ameaças externas?

Ameaças externas são possíveis perigos para a segurança da informação que surgem de fontes fora da organização.

Elas podem ser causadas por indivíduos ou organizações mal-intencionadas, como hackers, criminosos cibernéticos, concorrentes ou, até mesmo, governos estrangeiros.

Assim, os invasores podem explorar pontos fracos desconhecidos para obter acesso a informações confidenciais.

Malware

Malware é uma abreviação de "software malicioso", termo utilizado para descrever programas de computador projetados para causar danos ou comprometer a segurança de um sistema.
Esses programas geralmente são criados para roubar informações, espionar atividades, comprometer a segurança de um sistema ou roubar informações pessoais, como senhas e informações bancárias.

Engenharia Social

Engenharia social é considerada uma técnica de manipulação psicológica usada por hackers e criminosos cibernéticos para obter informações confidenciais ou acesso não autorizado a sistemas ou informações.
Em vez de usar técnicas de invasão direta, os hackers usam engenharia social para manipular usuários legítimos para que forneçam informações confidenciais, como senhas ou informações pessoais.

Phishing

Nesse tipo de ataque, o hacker geralmente envia um e-mail, mensagem de texto ou faz uma chamada telefônica fingindo ser uma empresa ou organização legítima, como um banco ou site de comércio eletrônico.
O objetivo do phishing é enganar a pessoa a fornecer informações confidenciais que possam ser usadas para roubar identidades, realizar transações fraudulentas ou outros tipos de atividades maliciosas.

Ransomware

Ransomwares buscam sequestrar o sistema de uma organização, exigindo o pagamento de um resgate para que o acesso ao sistema seja restabelecido.
Quando o ransomware é ativado, ele criptografa os arquivos no sistema da vítima, tornando-os inacessíveis.

Quais são as ameaças internas?

As ameaças internas são aquelas que surgem de dentro de uma organização, ou seja, de seus próprios funcionários, colaboradores ou parceiros de negócios.

Essas ameaças podem ser intencionais ou não e podem incluir, por exemplo, o uso indevido de informações confidenciais, o roubo de propriedade intelectual, a instalação de malware em sistemas corporativos, o acesso não autorizado a informações confidenciais ou a manipulação de dados.

Sabotagens e roubos

Roubos e sabotagens de dados e informações podem acontecer por meio de pessoas mal intencionadas que buscam prejudicar organizações deletando ou divulgando dados importantes e sensíveis.

Acessos não autorizados

Pessoas mal intencionadas podem utilizar vulnerabilidades nos sistemas da sua organização para obter acessos a informações que não possuem autorização. Dessa forma, esses dados podem correr riscos de serem comprometidos.

Perdas e vazamentos de dados

Perdas e vazamentos de dados ocorrem quando informações confidenciais de uma organização são expostas, roubadas ou perdidas. Isso pode incluir dados de clientes, informações financeiras, propriedade intelectual, dados pessoais de funcionários e outros tipos de informações sensíveis.

Conteúdos maliciosos

Uma pessoa despreparada sobre como agir em relação à proteção digital pode, acidentalmente, fazer download de conteúdos maliciosos que podem infectar sistemas e dispositivos.

Uso de dispositivos não autorizados

O uso de dispositivos pode permitir o acesso não autorizado a informações confidenciais e dados corporativos.

Quando usamos esses dispositivos pessoais para acessar e armazenar dados corporativos, eles podem inadvertidamente expor informações confidenciais a ameaças cibernéticas. Dispositivos não autorizados também podem conter malware ou vírus que podem infectar sistemas corporativos, colocando em risco toda a infraestrutura de TI.