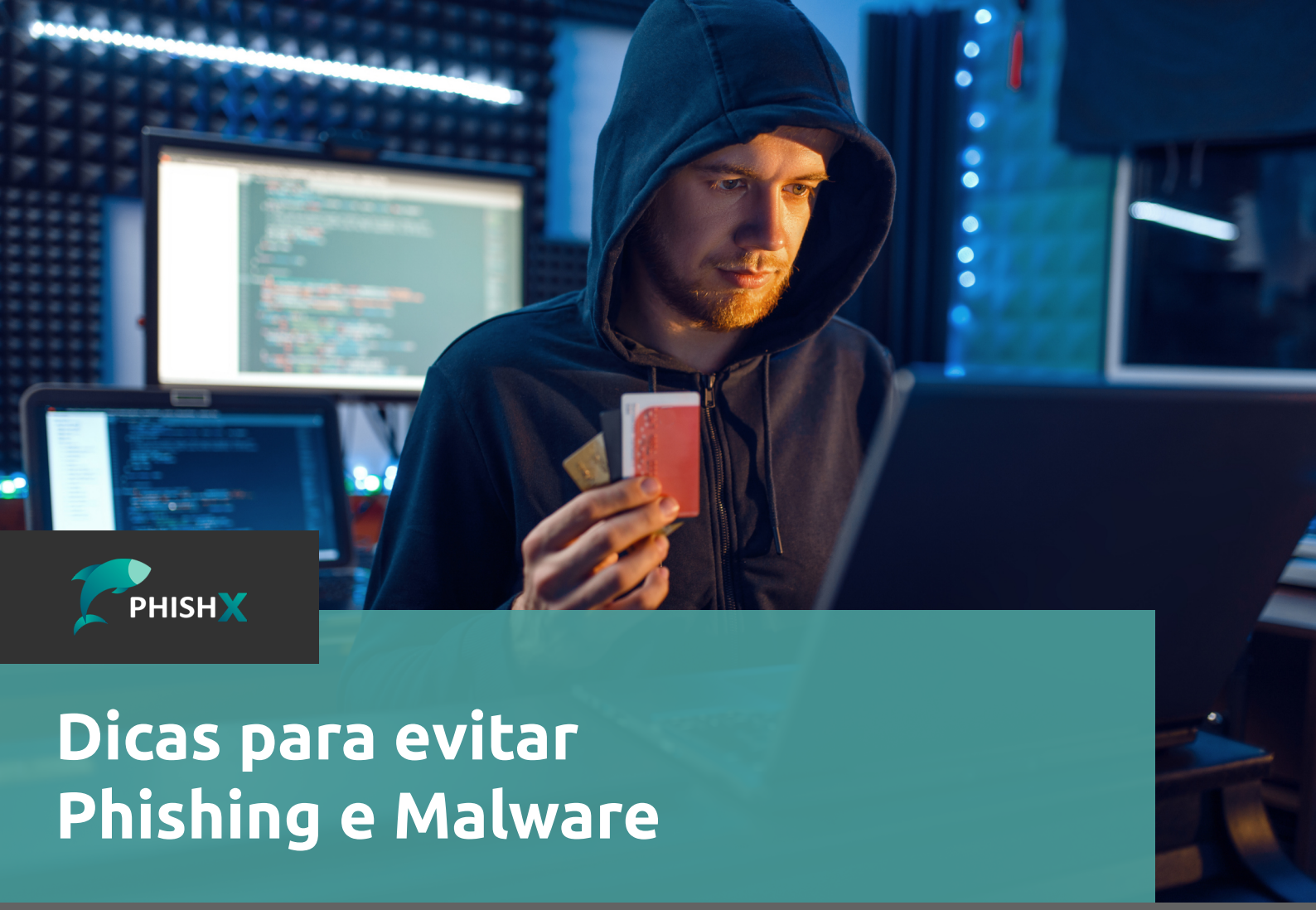

PHISHX

Dicas para evitar Phishing e Malware

Desconfie de mensagens suspeitas

O nome e o endereço do remetente que aparecem na mensagem podem ser facilmente modificados para mostrar informações falsas.

Empresas legítimas e bancos não enviam mensagens sem o devido cadastro e consentimento, sob hipótese alguma. Portanto, não acredite em mensagens de origens que você não tenha cadastrado e aprovado anteriormente.

Na dúvida, pegue uma segunda opinião. Acesse diretamente o site ou os canais oficiais de contato da empresa.

Desconfie da urgência e prazos

Provocar uma sensação de urgência ou medo é uma tática comum. Fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos.

Fique atento a mensagens, recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em links.

Desconfie de grandes promoções

Por mais tentador que pareça aquela viagem super barata, aquela promoção imperdível ou aquele e-mail cheio de perguntas que promete tirar todas as dúvidas com um simples "clique aqui", desconfie! É aí que se escondem as armadilhas, que colocam em risco você e seu colega de trabalho.

Lembre-se dos canais oficiais da empresa para divulgação de benefícios aos usuários.

Não execute arquivos desnecessários

Se você receber uma caixa de chocolates pelo correio de uma pessoa desconhecida, você a abriria e comeria tudo sem hesitação?

Provavelmente não. Da mesma forma, é importante ter cuidado quando uma pessoa desconhecida envia um e-mail suspeito contendo anexos e imagens.

Alguns sites e aplicativos permitem que você compartilhe arquivos facilmente com outros usuários. Muitos desses sites e aplicativos oferecem pouca proteção contra malware. Se você compartilhar ou fizer o download de arquivos usando esses métodos de compartilhamento, fique atento quanto à existência de malware. O malware pode se disfarçar como um filme, álbum, jogo ou programa popular.

Cuidados com links e anexos

Ao receber uma mensagem duvidosa, não acesse links e nem execute os arquivos anexos.

Verifique o link apresentado na mensagem.

Golpistas costumam usar técnicas para ofuscar o link real para o Phishing. Ao posicionar o mouse sobre o link, muitas vezes é possível ver o endereço real da página falsa ou código malicioso.

Se o endereço do link parecer estranho, não clique nele!

Leia o contrato com atenção

Parece algo chatinho de fazer – e, na verdade, é mesmo. Entretanto, é necessário. Alguns contratos ou termos, que aceitamos sem ler, autorizam que nossas informações salvas na máquina sejam encaminhadas para terceiros terem acesso.

E aí a gente sabe o que pode acontecer: invasão.