SEGURANÇA DA INFORMAÇÃO

eBook 3

Ataques de *Phishing*

Phishing é um tipo de ataque cibernético que tem como objetivo enganar as pessoas para que elas revelem informações confidenciais, como senhas e informações financeiras. Geralmente, os ataques de *phishing* são realizados por meio de mensagens de e-mail, mensagens de texto ou chamadas telefônicas que parecem ser legítimas, mas na verdade são fraudulentas.

Para identificar um ataque de *phishing*, é importante prestar atenção aos seguintes sinais:

- △ O remetente da mensagem é desconhecido ou o endereço de e-mail é suspeito.
- △ A mensagem pede que você revele informações confidenciais, como senhas ou informações financeiras.
- △ A mensagem tem erros gramaticais ou de ortografia.
- △ A mensagem tem um link suspeito que redireciona para um site falso.
- △ A mensagem pede que você faça algo imediatamente, como clicar em um link ou fornecer informações pessoais.

E para evitar ataques de phishing, é recomendado seguir estas boas práticas:

#1
Nunca revela informações confidenciais, como senhas ou informações financeiras, por e-mail ou mensagem de texto, a menos que você tenha certeza de que a mensagem é legítima.

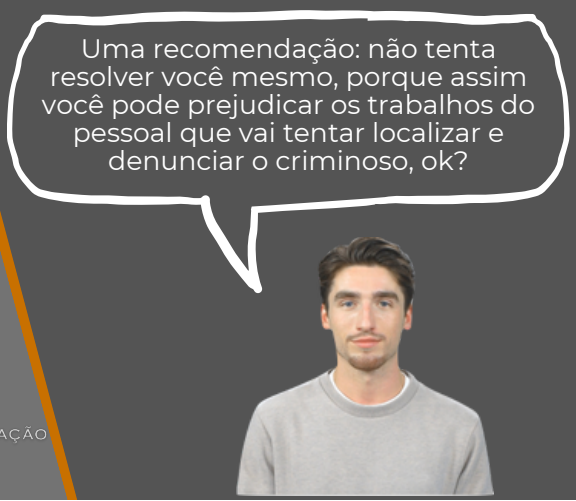
#2
Verifica sempre o endereço de e-mail do remetente e também se ele é legítimo antes de responder à mensagem.

#3
Nunca clica em links suspeitos em mensagens de e-mail ou mensagens de texto. Em vez disso, verifica o site manualmente digitando o endereço na barra de endereço do navegador.

#4
Mantém o software do computador e do celular atualizado e com as últimas correções de segurança.

#5
Usa um software ou app de segurança confiável e atualizado para proteger o teu computador e o celular contra malware e outras ameaças de segurança.

#6
Fica sempre atento a mensagens de e-mail ou mensagens de texto suspeitas. Se você achar que recebeu uma mensagem de phishing, exclui ela imediatamente, e denuncia o incidente à equipe de segurança de TI da tua empresa ou do provedor de serviços de e-mail.



A expressão phishing surgiu a partir da palavra em inglês "fishing", que significa "pescando". Ou seja, os criminosos utilizam esta técnica para "pescar" os dados das vítimas que "mordem o anzol" lançado pelo "pescador", que é quem executa um phishing.

Controle de Acessos

Para haver um controle de acessos, as empresas precisam ter sistemas de autenticação e autorização. E além do controle, a implementação adequada desses sistemas ajuda as empresas a cumprir regulamentações e padrões de segurança, como a Lei Geral de Proteção de Dados (LGPD).

As boas práticas incluem:

Identificar os usuários, que é primeira coisa que deve ser feita, e as funções que são desempenhadas dentro da organização.

Depois devem ser definidos os níveis de acesso com base nas funções dos usuários. Nem todos os usuários precisam de acesso a todas as informações confidenciais. Cada nível de acesso deve ser limitado apenas as finalidades necessárias para realizar as tarefas de trabalho.

Utilizar senhas fortes e incentivar os usuários a mudar as suas senhas regularmente é uma prática muito comum. E as senhas devem ser longas e complexas, misturando letras maiúsculas e minúsculas, números e caracteres especiais.

Implementar a autenticação multifator, que é usada para adicionar uma camada extra de segurança, onde os usuários têm que passar por duas ou mais etapas antes de acessar os sistemas.

Monitorar o acesso aos dados confidenciais também é essencial para detectar possíveis violações de segurança. E os registros de acesso também costumam ser armazenados e revisados regularmente.

Revogar o acesso quando um funcionário deixa a empresa ou muda de cargo é importante, para que não seja possível o acesso aos dados confidenciais. E também é comum que, além da revogação, o acesso não seja permitido por mais tempo do que o necessário.