***O ATAQUE PHISHING***

O ataque de phishing é uma forma de fraude online em que os criminosos se passam por uma entidade confiável para obter informações sensíveis dos usuários, como senhas, números de cartão de crédito ou informações pessoais. Este ataque geralmente é realizado por meio de e-mails falsos, mensagens de texto, sites ou até mesmo ligações telefônicas.

Os ataques de phishing são projetados para enganar as pessoas e fazê-las acreditar que estão interagindo com uma organização legítima, como um banco, uma empresa conhecida ou um serviço online popular. Os golpistas geralmente tentam criar um senso de urgência ou medo para incentivar as vítimas a revelarem suas informações.

Existem várias técnicas de phishing, como:

E-mails de phishing: os criminosos enviam e-mails falsos que se parecem com os de empresas legítimas. Esses e-mails geralmente solicitam que os usuários cliquem em um link e insiram suas informações pessoais em um site falso.

Websites de phishing: os golpistas criam sites falsos que se assemelham aos legítimos, como páginas de login de bancos ou de serviços de e-commerce. Os usuários são levados a fornecer suas informações pessoais, que são então roubadas pelos criminosos.

Mensagens de texto de phishing: os fraudadores também podem enviar mensagens de texto falsas que solicitam informações pessoais ou levam os usuários a clicar em links maliciosos.

Engenharia social: os ataques de phishing também podem envolver chamadas telefônicas, em que os criminosos se passam por representantes de empresas conhecidas e solicitam informações pessoais ou financeiras.

Proteger-se contra-ataques de phishing envolve estar atento e tomar algumas precauções, como nunca clicar em links suspeitos ou compartilhar informações confidenciais por meio de e-mails não solicitados. É importante verificar a autenticidade dos sites, verificar os remetentes de e-mails e manter os softwares e sistemas atualizados para evitar possíveis vulnerabilidades que possam ser exploradas pelos golpistas.