Glossário de Segurança Mobile

Phishing, malware, ransomware... O DFNDR Lab explica o significado de cada termo do universo de segurança mobile.

Adware
Tipo de software que excessivamente exibe propagandas e anúncios enquanto o usuário usa o dispositivo.

Carder
Aquele que compra e vende na internet dados de cartão de crédito roubados através de golpes de phishing ou de ataques a sites de varejo.

Ciberataque
Qualquer atividade ilícita realizada na internet ou por meio de um dispositivo eletrônico. Tais atividades incluem fraude, roubo de identidade, phishing etc.

Crimeware
Qualquer software criado para praticar crimes digitais e, assim, obter ganho financeiro.

DoS / Denial of Service
Método de ataque capaz de desligar dispositivos ou redes e impedir que usuários acessem certos serviços.

Dropper
Arquivo executável que insere diferentes tipos de vírus em um dispositivo.

Engenharia Social
Método usado por hackers para espalhar links maliciosos e realizar ataques de maneira indireta, em geral por meio de pessoas de confiança da vítima, como familiares e amigos. A vítima fica mais inclinada a aceitar e clicar em links se eles vierem de quem ela confia.

Ferramenta de Hacking
Software ou instrumento usado por um hacker para realizar ações ilegais ou sem autorização.

Golpe
Qualquer atividade em que um usuário é levado a fornecer dinheiro ou dados financeiros a partir de falsas promessas.

Golpe do SMS pago
SMS que oferece um serviço falso e exige pagamento para que o usuário conclua a assinatura.

Hacker
Aquele que acessa um dispositivo, software ou rede de computadores de forma ilegal ou sem autorização.

Hijacker
Softwarea que alteram as configurações do navegador para modificar a página principal ou site de busca padrão selecionado previamente pelo usuário.

Hijacking
Tipo de ataque em que o invasor assume o controle da comunicação entre duas entidades e simula ser uma delas.

Hoax
Mensagem alarmista com conteúdo falso – como um alerta de vírus – criado para enganar o usuário.

Keylogger
Tipo de trojan que é capaz de coletar, registrar e até mesmo publicar tudo que o usuário digitou em seu teclado.

Link malicioso
Sites criados com propósito malicioso, como enganar o usuário ou roubar informações. Contemplam bad ads, golpes de phishing, notícias falsas, sites de malware etc.

Malware
Todos os softwares que contêm um código malicioso, como vírus, trojan ou worm.

Notícias falsas
Conteúdos escritos e publicados de maneira a se parecerem com notícias reais com a intenção de enganar o usuário para obter vantagens diversas.

Password stealer
Software que coleta e salva dados confidenciais do usuário, como senhas, utilizando um keylogger ou outro malware.

Payload
Partes de código dentro de malwares que realizam ações em dispositivos infectados, como roubo de dados, remoção de arquivos etc.

Phishing
Armadilhas criadas para induzir o usuário a compartilhar seus dados pessoais ou financeiros, como senhas, número de celular e dados do cartão de crédito.

Phishing bancário
Sites falsos iguais às páginas de instituições bancárias criados para enganar usuários e roubar suas credenciais do banco, como tokens, senha, número da conta, dados de cartão de crédito etc.

Phishing de premiação falsa
Tipo de golpe que diz que o usuário ganhou um prêmio. Normalmente, depois do clique, ele é obrigado a baixar um app, fornecer dados pessoais ou se inscrever em um serviço pago.

Phishing de malware
Tipo de ataque de phishing em que o usuário é induzido a clicar em um link contendo um malware que pode danificar seu dispositivo ou roubar dados pessoais.

Phishing de perfil falso
Perfis falsos criados em redes sociais para persuadir ou redirecionar usuários para outros ataques que podem acarretar no roubo de seus dados pessoais e financeiros.

Phishing de redes sociais
Ataques criados para roubar credenciais das redes sociais a fim de invadir a conta do usuário e usá-la com propósito malicioso.

Phishing de serviços falsos
Página que oferece um serviço em que o usuário é obrigado a fornecer seus dados, instalar algum app ou se inscrever em outro serviço pago para usufruir da oferta, mas ao final não recebe o prometido.

Phishing via aplicativo de mensagens
Tipo de página falsa que obriga o usuário a fornecer dados pessoais e compartilhar um link com seus contatos em mensageiros como WhatsApp.

Publicidade enganosa (Bad Ads)
Páginas ou pop-ups com mensagens que enganam o usuário, por exemplo, afirmando que o celular tem vírus, para forçá-lo a assinar serviços ou instalar aplicativos.

Ransomware
Software que impede o usuário de acessar seu dispositivo, muitas vezes através de criptografia, e só libera o acesso mediante pagamento de resgate.

Riskware
Software legítimo com vulnerabilidades que podem ser exploradas por hackers com propósitos maliciosos.

Scammer
Alguém que finge ser um usuário legítimo de uma plataforma para convencer outras pessoas a enviar dinheiro, informações pessoais ou financeiras e a instalar arquivos maliciosos.

Site com malware
Link enganoso criado para induzir o usuário a instalar um malware que pode danificar seu dispositivo ou roubar dados pessoais.

Spammer
Aquele que é responsável por desenvolver um software ou por enviar um enorme número de e-mails com propósito malicioso, como golpes de phishing ou malware.

Spyware
Software que recolhe informações pessoais, como histórico de navegação, preferências e interesses, e usa o que coletou sem consentimento do usuário.

Trojan
Software que simula executar uma atividade, mas na verdade faz outra. Geralmente, a ação é maliciosa e pode roubar dados ou redirecionar o usuário para sites. Também é conhecido como Cavalo de Troia.

Trojan bancário
Tipo de trojan criado para roubar dados bancários, como as credenciais de clientes de cartão de crédito, em plataformas online de bancos ou de pagamentos.

Vírus
Tipo de malware que se insere dentro de um arquivo ou software executável e pode causar diversos problemas como tornar o sistema lento ou danificar e modificar arquivos.

Vulnerabilidade
Uma falha ou erro em um software ou sistema que pode permitir a ação de um hacker com propósito malicioso.

Worm
Malware autônomo muito parecido com o vírus, mas que pode se autorreplicar e se propagar através da rede para outros dispositivos sem a interferência de um humano.