Um hacker é alguém que tem habilidades avançadas em computação e segurança cibernética. Essas pessoas geralmente têm um profundo conhecimento de sistemas de computador e redes, e usam essas habilidades para **explorar e melhorar a segurança de sistemas**. Hackers podem ser classificados em diferentes categorias, como hackers éticos (também conhecidos como white hat hackers), que usam suas habilidades para proteger sistemas e descobrir vulnerabilidades antes que sejam exploradas por indivíduos mal-intencionados; hackers ativistas (também conhecidos como hacktivistas), que usam suas habilidades para promover causas políticas ou sociais; e hackers maliciosos (também conhecidos como black hat hackers), que usam suas habilidades para obter acesso não autorizado a sistemas e prejudicar outros.

Hackers éticos, também conhecidos como white hat hackers, são profissionais de segurança cibernética que usam suas habilidades em computação para identificar e corrigir vulnerabilidades em sistemas de computador e redes. Eles desempenham um papel importante na proteção da segurança digital, atuando como defensores dos sistemas e ajudando a fortalecer a infraestrutura de segurança.

Os hackers éticos são contratados por empresas, organizações governamentais e outras entidades para realizar testes de penetração, também conhecidos como pentests. Eles procuram ativamente por brechas e fraquezas nos sistemas, a fim de identificar e corrigir possíveis pontos de entrada para ataques maliciosos. Os pentests são realizados de forma controlada e legal, com o consentimento do proprietário do sistema.

A principal motivação dos hackers éticos é ajudar a melhorar a segurança cibernética. Eles trabalham em estreita colaboração com empresas para fortalecer suas defesas, fornecendo recomendações sobre como mitigar as vulnerabilidades encontradas. Ao revelar falhas de segurança, os hackers éticos ajudam as organizações a se protegerem contra ataques maliciosos e a manter a confiança dos clientes.

Muitos hackers éticos possuem certificações reconhecidas, como Certified Ethical Hacker (CEH) ou Offensive Security Certified Professional (OSCP). Essas certificações atestam seu conhecimento e habilidades em testes de penetração e demonstram seu compromisso com a ética e a legalidade.

É importante ressaltar que os hackers éticos operam dentro dos limites legais e éticos. Eles seguem um código de conduta que define suas atividades, evitando danos, invasão de privacidade e roubo de informações. Seu objetivo é proteger os sistemas e contribuir para um ambiente digital mais seguro.

Os hackers ativistas, também conhecidos como **hacktivistas**, são indivíduos ou grupos que usam suas habilidades em computação para **promover causas políticas, sociais ou ideológicas**. Eles utilizam técnicas de hacking e ciberativismo para chamar a atenção para questões específicas, divulgar informações, expor práticas questionáveis ou lutar por mudanças em diversos âmbitos da sociedade.

Os hacktivistas geralmente se envolvem em atividades como:

**Desfiguração de websites:** Eles invadem sites de organizações, governos ou empresas para modificar seu conteúdo, muitas vezes deixando mensagens ou símbolos relacionados à causa que estão defendendo.

**Vazamento de informações:** Os hacktivistas podem expor informações confidenciais, como e-mails, documentos ou dados sensíveis, com o objetivo de revelar ações consideradas antiéticas, corruptas ou prejudiciais ao interesse público.

**Ataques distribuídos de negação de serviço (DDoS):** Esses ataques sobrecarregam um site ou serviço online com tráfego excessivo, tornando-o inacessível. Os hacktivistas podem usar essa técnica para interromper as operações de uma organização ou para protestar contra suas práticas.

**Ações de conscientização:** Os hacktivistas buscam aumentar a conscientização sobre questões específicas, divulgando informações por meio de vazamentos, ataques cibernéticos ou propaganda online.

**Defesa de direitos digitais:** Muitos hacktivistas lutam pela privacidade, liberdade de expressão e direitos digitais, atuando contra leis e políticas que consideram ameaças à liberdade na internet.

É importante ressaltar que as ações dos hacktivistas **nem sempre são legais** e podem resultar em consequências jurídicas. Embora alguns deles se concentrem em causas justas e tenham como objetivo promover mudanças positivas, outros podem se envolver em atividades ilegais e prejudiciais.

Os hacktivistas são conhecidos por usar a internet como uma plataforma para ampliar sua mensagem e alcançar um público maior. Suas atividades têm o potencial de influenciar debates públicos, expor práticas questionáveis e moldar a opinião pública sobre questões sociais e políticas.

Hackers maliciosos, também conhecidos como black hat hackers, são indivíduos que usam suas habilidades em computação para realizar atividades ilegais e prejudiciais. Eles exploram vulnerabilidades em sistemas de computador e redes com o objetivo de obter acesso não autorizado, roubar informações confidenciais, causar danos ou obter ganhos financeiros ilícitos.

Os hackers maliciosos estão envolvidos em uma ampla gama de atividades prejudiciais, incluindo:

Roubo de informações: Eles procuram obter acesso a dados confidenciais, como informações pessoais, números de cartão de crédito, senhas e segredos comerciais, que podem ser vendidos no mercado negro ou usados para extorsão.

Ataques de negação de serviço (DoS) e extorsão: Os hackers maliciosos podem sobrecarregar um site ou serviço online, tornando-o inacessível para usuários legítimos. Eles podem exigir um resgate (ransom) para interromper o ataque ou ameaçar continuar prejudicando as operações.

Distribuição de malware: Eles desenvolvem e distribuem softwares maliciosos, como vírus, worms, cavalos de Troia e ransomware, com o objetivo de infectar sistemas e roubar informações, danificar arquivos ou obter controle remoto dos dispositivos comprometidos.

Phishing e engenharia social: Os hackers maliciosos enviam e-mails ou mensagens falsas, fingindo serem legítimas, para enganar as pessoas e levá-las a revelar informações confidenciais, como senhas, números de cartão de crédito ou dados pessoais.

Invasões de sistemas: Eles exploram vulnerabilidades em sistemas operacionais, aplicativos ou redes para obter acesso não autorizado a servidores, bancos de dados ou infraestruturas críticas, comprometendo a segurança e a privacidade dos sistemas.

É importante ressaltar que as atividades dos hackers maliciosos são ilegais e podem levar a sérias consequências legais. Eles operam fora dos limites éticos e são motivados principalmente por ganhos pessoais, prejudicando indivíduos, empresas e até mesmo infraestruturas governamentais.

Contrariamente aos hackers éticos, os hackers maliciosos não têm preocupação com a segurança dos sistemas e geralmente têm intenções prejudiciais. Portanto, é fundamental adotar medidas de segurança robustas para proteger sistemas e redes contra ataques maliciosos.

Na prática, a diferença entre um hacker malicioso e um cracker é sutil e muitas vezes os termos são usados de forma intercambiável. No entanto, algumas definições sugerem uma distinção com base nas motivações e nas atividades específicas.

Geralmente, o termo "hacker malicioso" ou "black hat hacker" é usado para se referir a indivíduos que exploram vulnerabilidades em sistemas de computador e redes com intenções prejudiciais. Esses hackers estão envolvidos em atividades ilegais, como roubo de informações, distribuição de malware, invasões de sistemas e outros ataques cibernéticos. Sua motivação principal é obter ganhos pessoais, causar danos ou violar a privacidade e a segurança de terceiros.

Já o termo "cracker" é frequentemente utilizado para descrever indivíduos com habilidades semelhantes que se concentram em quebrar sistemas de segurança, superar restrições de licenciamento de software ou contornar medidas de proteção digital para obter acesso não autorizado a recursos protegidos. Os crackers são frequentemente associados a atividades como a pirataria de software, a quebra de senhas, a clonagem de cartões de crédito e outras práticas ilícitas.

Em resumo, enquanto o termo "hacker malicioso" está mais relacionado a indivíduos que realizam atividades ilegais com motivações prejudiciais, o termo "cracker" pode se referir a pessoas que se especializam em contornar sistemas de segurança e proteção para obter acesso não autorizado, independentemente de suas intenções. No entanto, é importante observar que a distinção entre os termos pode variar e que o uso dos mesmos pode ser ambíguo na prática.