**Hackers e Crackers: quais as diferenças entre eles?**

Um ataque lançado geralmente a partir de um computador recorrendo ao método de intrusão e que tem como finalidade adquirir, explorar, perturbar, romper, negar, degradar ou destruir informação constante em computadores ou em redes de computadores, em sistemas e equipamentos eletrónicos ligados a outros equipamentos ou sistemas ou que partilham a mesma estrutura de energia ou o mesmo espaço de emissão eletromagnética, bem como os próprios computadores,

redes de computadores, sistemas e equipamentos

Muito utilizados na área da informática, termos como “**hackers” e “crackers**” servem para se referir a pessoas com habilidade e conhecimentos avançados em computadores e dispositivos móveis.

De modo geral, eles **sabem encontrar brechas em sistemas operacionais e softwares**. Mas as semelhanças acabam aí. Cada um desses “grupos” utiliza seus conhecimentos para **alcançar objetivos distintos.**

No entanto, não é raro ver pessoas que não dominam o vocabulário da computação **confundir os termos e se referir a eles de forma errada.** Para não fazer essa confusão, confira as diferenças entre hackers e crackers logo abaixo:

**Hackers**

São aqueles indivíduos que possuem **conhecimentos profundos de informática e fazem uso deles de forma positiva.** **Os hackers dedicam boa parte do seu tempo a conhecer e modificar softwares, hardwares e redes de computadores**. Seus conhecimentos são utilizados para obter **soluções de segurança**, além de desenvolver novas funcionalidades no mundo da computação.

O que isso significa? Que eles não são criminosos, como se costuma ver por aí em sites e até mesmo na mídia tradicional. Na verdade, trata-se do oposto: **os hackers utilizam sua sabedoria de forma benéfica, sem tentar levar vantagem.**

No entanto, assim como na vida, algumas pessoas se valem de práticas duvidosas para alcançar o que é considerado um **“bem maior”. Por isso, os hackers também se dividem em subgrupos, que são:**

**White Hats (Chapéu Branco)**

São os **hackers interessados em segurança** e que, em boa parte das vezes, utilizam suas habilidades em favor de empresas. **Esses hackers são 100% éticos em suas ações**. Nesse sentido, eles **são contratados por empresas** para ocupar cargos **de analista de sistemas, especialistas em TI,** entre outros.

Volta e meia, navegadores, softwares e sistemas operacionais lançam pacotes de atualizações para corrigir **brechas de segurança**. Normalmente, essas brechas de **segurança são descobertas pelos hackers White Hats.**

**Black Hats (Chapéu Preto)**

**São os hackers que burlam sistemas e são especializados em invasões maliciosas de sites**, quase sempre com **intenções duvidosas**. Esses também são malvistos por seus **colegas, inclusive sendo considerados tão criminosos quanto os crackers.**

**Gray Hats (Chapéu Cinza)**

Os gray hats, assim como os white hats, **são muito bem-intencionados**. Contudo, acabam se perdendo um pouco na ansiedade de fazer **valer sua vontade de ajudar**, usando ações que podem ser eticamente questionáveis. Um exemplo é quando eles **realizam testes de segurança em uma rede de computadores antes de pedir permissão aos envolvidos.**

**Crackers**

Quanto aos crackers, eles utilizam seus grandes conhecimentos em informática de forma **menos honesta: quebrando (cracking) sistemas de segurança de software**s para ter alguma **vantagem financeira** lá na frente. Esse tipo de **atividade é considerado ilegal** e, por isso, os **crackers são vistos como criminosos.**

O termo usado para denominá-los foi **cunhado pelos próprios hackers**, por volta de 1985, com o objetivo de diferenciar, para a mídia e para os leigos, as atividades exercidas por cada um dos grupos. **Mesmo depois de tanto tempo, ainda encontramos muita gente confundindo os termos.**

**As redes públicas são fontes de dados pessoais bastante ricas**, por isso são o principal foco dos **crackers.** Por meio delas, eles conseguem **roubar senhas e outras informações de quem acessa seus serviços online.**

Desse modo, ao utilizar uma rede pública, é importante evitar inserir informações como senhas, CPF e endereços. A dica nesse caso é utilizar a internet da sua operadora de telefonia móvel. Quando indisponível, priorize as redes que exigem senha, já que oferecem menor risco.

**Tratando-se de crime informático**, ele pode ser originado de diversas formas: distribuição de material de pornografia infantil; *phishing* e fraudes contra bancos; mensagens difamatórias em sites de relacionamento; violação de propriedade intelectual; espionagem; ilícitos econômicos; sabotagem e extorsão; uso não autorizado de sistemas; manipulação de dados; pichação informática ou *defacement (*esta não é uma lista exaustiva e existem várias outras modalidades).