What is a Hacker and How Does Someone Become One?

When someone says “hacker” what’s the first thing that comes to mind? I’d be willing to bet that you thought of someone sitting behind a computer committing crimes through malicious activity, Did you know that the term “hacker” didn’t always have a negative connotation? Hackers are usually very skilled in programming and computer networking, and they have a good understanding of security systems and how to exploit them. The term “hacker” actually describes both the cyber-criminal and the “good guy” technological experts.To differentiate what type of hacker one is, they are divided into different categories.

Types of Hackers

Hackers are categorized into 3 main types: white hat, black hat, and gray hat hackers. Although these different types of hackers go about it in very different ways, they all share one common goal: to find and exploit weaknesses in computer systems. The main difference between the 3 types of hackers is their motivation when they break into computer systems. Some are motivated by the challenge, others by the opportunity to make money, and still others by the desire to cause mischief or mayhem.

“White hat” hackers are ethical security hackers, or the “good guys.” Their motivation typically stems from their ethics and wanting to help company’s build stronger security systems.

Many of them work as security consultants, they use their skills to find security vulnerabilities and help companies fix them before they can be exploited by the bad guys. They may also use their skills to expose security flaws in order to pressure companies to fix them.

“Black hat” hackers are the ones you typically think of when you hear the word “hacker.” They are the bad guys, the criminal hackers. They commit cybercrime usually for financial gain or to cause chaos through cyber espionage by exploiting security vulnerabilities and causing damage. They use their skills to steal sensitive information, commit identity theft, or launch attacks that disrupt websites or cripple computer systems.

Then, there are the “gray hat” hackers, who fall somewhere in between white hat and black hat hackers. Many of them believe they need to prove how unsafe the internet is for companies and individuals with the amount of data leakage.They use their skills, without consent, to find and exploit security vulnerabilities. Gray hat hackers don’t have malicious intent but they do often demand payment in exchange for full details of what they uncovered.

Sub-types of Hackers

Although most all hackers fall into one of the three categories listed above: white, black, or gray hat hackers, there are other sub-types of hackers: green hat, blue hat, and red hat.

“Green hat” hackers are new hackers, thus they’re

inexperienced and lack technical skills. They may or may not have malicious intentions but they can be dangerous by accidentally causing damage whilst performing various cyber-attack techniques as they learn and develop new skills.

“Blue hat” hackers are people who are employed by a company or organization to look for any vulnerabilities or bugs within their security systems and/or soon-to-be released software. They look for vulnerabilities with a security system by conducting a penetration test, or pen test. A pen test is an authorized cyber-attack on a computer system conducted to evaluate the security of the system. Sometimes, a blue hat hacker references someone that is seeking revenge against someone; it may be a particular person, a former employer, or an entire country.

Lastly, there are “red hat” hackers, AKA vigilante hackers. Red hat hackers work to fight back against black hat hackers by taking matters into their own hands and infiltrating the black hat communities. Although noble, these hackers often use unethical or illegal methods to take down black hat hackers.

Which type of hacker are you?

Becoming a Hacker

How does one become a hacker? There’s no school teaching someone how to become a hacker. You can take courses teaching you about computer basics, the systems, and programming but hacking comes from learning to manipulate systems and programs into doing something they were not designed to do.

Most hackers:

- Are self-taught, and they are always looking for ways to improve their skills.
- Learn by trial and error; they are constantly experimenting with new techniques and tools.

- Are quick thinkers who can come up with innovative solutions to difficult problems.
- Are experts at finding and exploiting security vulnerabilities, and they have a deep understanding of how computer systems work.
- Are creative problem-solvers who are always looking for new challenges.

In conclusion, there are many different types of hackers out there. Some hack for good, some for bad, and some for personal gain. Whatever their motivation for hacking, some hackers can have a significant impact on our lives. They can cause financial damage, stress, and even jeopardize our safety. Be sure to stay informed and keep your computer security up-to-date to protect yourself from the dangers of the internet.