HACKING

Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorised access to or control over computer network security systems for some illicit purpose. A commonly used definition of hacking is the act of compromising digital devices and networks through unauthorized access to an account or computer system. Hacking is not always a malicious act, but it is most commonly associated with illegal activity and data theft by cyber criminals. Hacking refers to the misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activity.

Hacking first appeared as a term in the 1970s but became more popular through the next decade. An article in a 1980 edition of Psychology Today ran the headline "The Hacker Papers" in an exploration of computer usage's addictive nature. Two years later, two movies, Tron and War Games, were released, in which the lead characters set about hacking into computer systems, which introduced the concept of hacking to a wide audience and as a potential national security risk. Sure enough, later that year, a group of teenagers cracked the computer systems of major organizations like Los Alamos National Laboratory, Security Pacific Bank, and Sloan-Kettering Cancer Centre. A Newsweek article covering the event became the first to use the word "hacker" in the negative light it now holds. This event also led Congress to pass several bills around computer crimes, but that did not stop the number of high-profile attacks on corporate and government systems. Of course, the concept of hacking has spiralled with the release of the public internet, which has led to far more opportunities and more lucrative rewards for hacking activity. This saw techniques evolve and increase in sophistication and gave birth to a wide range of types of hacking and hackers.

A traditional view of hackers is a lone rogue programmer who is highly skilled in coding and modifying computer software and hardware systems. But this narrow view does not cover the true technical nature of hacking. Hackers are increasingly growing in sophistication, using stealthy attack methods designed to go completely unnoticed by cybersecurity software and IT teams. They are also highly skilled in creating attack vectors that trick users into opening malicious attachments or links and freely giving up their sensitive personal data. As a result, modern-day hacking involves far more than just an angry kid in their bedroom. It is a multibillion-dollar industry with extremely sophisticated and successful techniques. To better describe hacking, one needs to first understand hackers. One can easily assume them to be intelligent and highly skilled in computers. In fact, breaking a security system requires more intelligence and expertise than actually creating one. There are no hard and fast rules whereby we can categorize hackers into neat compartments. However, in general computer parlance, we call them white hats, black hats and grey hats.

Hacking: Motives and Types

There are typically four key drivers that lead to bad actors hacking websites or systems: (1) financial gain through the theft of credit card details or by defrauding financial services, (2) corporate espionage, (3) to gain notoriety or respect for their hacking talents, and (4) state-sponsored hacking that aims to steal business information and national intelligence. On top of that, there are politically motivated hackers—or hacktivists—who aim to raise public attention by leaking sensitive information, such as Anonymous, LulzSec, and WikiLeaks.

White Hat: White hat professionals hack to check their own security systems to make it more hack-proof. In most cases, they are part of the same organisation. White hat hackers can be seen as the “good guys” who attempt to prevent the success of black hat hackers through proactive hacking. They use their technical skills to break into systems to assess and test the level of network security, also known as ethical hacking. This helps expose vulnerabilities in systems before black hat hackers can detect and exploit them. The techniques white hat hackers use are similar to or even identical to those of black hat hackers, but these individuals are hired by organizations to test and discover potential holes in their security defences.

Black Hat: Black hat hackers hack to take control over the system for personal gains. They can destroy, steal or even prevent authorized users from accessing the system. They do this by finding loopholes and weaknesses in the system. Some computer experts call them crackers instead of hackers. They are the "bad guys" of the hacking scene. They go out of their way to discover vulnerabilities in computer systems and software to exploit them for financial gain or for more malicious purposes, such as to gain reputation, carry out corporate espionage, or as part of a nation-state hacking campaign. These individuals’ actions can inflict serious damage on both computer users and the organizations they work for. They can steal sensitive personal information, compromise computer and financial systems, and alter or take down the functionality of websites and critical networks.

Grey Hat: Grey hat hackers comprise curious people who have just about enough computer language skills to enable them to hack a system to locate potential loopholes in the network security system. Grey hats differ from black hats in the sense that the former notify the admin of the network system about the weaknesses discovered in the system, whereas the latter is only looking for personal gains. They sit somewhere between the good and the bad guys. Unlike black hat hackers, they attempt to violate standards and principles but without intending to do harm or gain financially. Their actions are typically carried out for the common good. For example, they may exploit a vulnerability to raise awareness that it exists, but unlike white hat hackers, they do so publicly. This alerts malicious actors to the existence of the vulnerability. All kinds of hacking are considered illegal barring the work done by white hat hackers.