# CRACKING THE CODE

## < WHAT IS ETHICAL HACKING? >

KING UNIVERSITY

ESTABLISHED IN 1867

# TABLE OF CONTENTS

# CRACKING THE CODE

## < WHAT IS ETHICAL HACKING? >

The word "hacking" probably conjures images of criminals in the movies or data breaches that fill the news. The truth is, though, there are hackers who protect us every day. These ethical hackers, as they are known, use many of the same skills criminal hackers use to find weak points in systems, and they are part of an ever-growing profession of cybersecurity experts who work to protect organizations from cybercriminals.

As data breaches become more common, organizations have begun to enhance their cybersecurity by hiring professionals who are well versed in hacking and locating insufficiencies in the systems that protect our data. Ethical hacking can prevent major cyberattacks and protect organizations and individuals from those with malicious intent.

# WHAT IS HACKING?

Hacking is defined as accessing a computer system or network without the authorization to do so. In today's cybersecurity landscape, this definition doesn't consider ethical hacking. Ethical hacking is hacking the administrators of systems or networks consent to in order to protect their data and technology.

There are many methods of hacking used by cybersecurity professionals and criminals alike. Technology giant Cisco detailed some of the most common types of hacking, which include:

- **MALWARE:** Victims may download viruses, worms, and spyware without even realizing it. All it could take is clicking on the wrong link for malware to enter a user's system. Malware can embed itself in a hard drive, install additional malicious software, and block access to certain parts of a network.

- **PHISHING:** Similar to bait on a hook, phishing misleads the victim into thinking an email is from a trusted source. When the victim clicks on a link within that email, a virus is downloaded to the computer that gives hackers access to personal data.

- **MAN-IN-THE-MIDDLE ATTACK (MitM):** When a user connects to the internet via Wi-Fi, information flows between the user and the network. With this technique, hackers interrupt that flow of information by inserting themselves in the middle.

- **DENIAL-OF-SERVICE (DoS):** DoS attacks are when hackers use software to overwhelm a set of servers, leading them to crash. When hackers target multiple servers from multiple devices, it's known as a distributed denial of service (DDoS).

- **SQL INJECTION:** With this method, hackers insert a harmful script in the coding language of a network or server. The script then instructs the server to supply information and data back to the hackers.

These are just some of the many different types of cyberattacks. Just as the kinds of breaches vary, so do unethical hackers' reasons for attacking. A hacker's motivations are what we use to define which type of hacker they are.

# WHAT ARE THE DIFFERENT TYPES OF HACKERS?

Hackers are organized into different groups segmented by their ultimate goal. Many hackers are described using colored hats, referencing the practice of referring to heroes as white hats and criminals as black hats. In old Western movies, the hero would often wear a white cowboy hat, while the villain would wear a black one. As the effects of a cyberattack can be far reaching and damaging, hackers can truly be heroes or villains.

Below, we'll focus on some of the main types of hackers.

## WHITE HAT HACKERS

White hat hackers have an ethical purpose to their work. They work with the permission of system administrators to find weak points in organizations' servers. They communicate their findings directly to the organization so that it can improve its cyber defenses. White hat hackers use the same methods as criminal hackers to probe for security vulnerabilities, but they don't do so maliciously. Many employers across multiple industries hire white hat hackers to test and improve their cybersecurity defenses.

## BLACK HAT HACKERS

Black hat hackers break into servers and networks to steal data and use that information for criminal purposes. The U.S. government considers breaking into a server or network without authorization a crime. Those who are found guilty of illegal hacking could face steep fines and a possible prison sentence.

## GRAY HAT HACKERS

Gray hat hackers work in the middle ground between white and black hat hackers. They uncover cybersecurity cracks without consent from an organization but also without criminal intent. Their goal may be to expose the vulnerability of an organization's systems without being asked.

### BLUE HAT HACKERS

Blue hat hackers are hired to test for bugs and security vulnerabilities in unreleased software. Their intent is to precisely identify weaknesses before software goes public. The term blue hat hacker came from Microsoft's blue ID cards.

### SCRIPT KIDDIE

Script kiddies are unskilled hackers who use tools from other hackers to deface webpages and leak personal data. Their motivation is often to sharpen their hacking skills or to simply have fun watching the havoc their hacking causes.

### HACKTIVIST

People who conduct hacks for a political or social cause are known as hacktivists. Hacktivists often feel their mission justifies the crime of hacking. They have a message or purpose that they want to convey with the act of hacking.

These diverse hackers make up the world of cyberattacks and cybersecurity. Understanding the motives of those wishing to exploit vulnerabilities and how they attack allows ethical hackers to carry out their mission of protecting individuals and organizations.

# WHY IS ETHICAL HACKING IMPORTANT?

In the fight against a long list of cybersecurity threats, ethical hacking plays a huge role. Data breaches are becoming more common and costly every year. In its latest report, the Center for Strategic and International Studies stated that cybercrime costs an estimated $600 billion per year globally. Most businesses can't afford to absorb fines, loss of trust, and other negative impacts of data breaches, which has made ethical hacking jobs a valuable component of cyber defense.

Millions of hacking attempts are made on servers every day. In an interview with the Pew Charitable Trusts, Missouri's top information security administrator said the state's cybersecurity defense system "blocks 95 million" attempts to access state servers per day.

***Missouri's cybersecurity defense system is reported to block 95 million attempts to access the state servers every day.***

# WHAT ARE ETHICAL HACKERS TARGETING?

Ethical hackers are always looking to stay one step ahead of criminal hackers by identifying cybersecurity cracks and errors in code. It's an ethical hacker's job to find cybersecurity vulnerabilities and patch them before they can be exploited by criminals. Every piece of software that's used by an organization could have a vulnerability within it. That means that ethical hackers must stay vigilant in their search for errors.

Vulnerabilities can exist for organizations and individuals in a variety of devices and places. For example, a report from Deloitte states internet of things (IoT) devices are one of the biggest cybersecurity risks for an organization. IoT devices are appliances, personal devices, and vehicles that contain software, sensors, and other technology that connect to the internet. They communicate and share sometimes sensitive data with other internet-connected devices. Unfortunately, this can often leave data and devices susceptible to hackers as information is stored and exchanged often.

## < HOW DO ETHICAL HACKERS OPERATE? >

On a day-to-day basis, many ethical hackers conduct probes known as penetration testing on their employer's servers and networks. Penetration testing simulates cyberattacks to check for points of weakness. Here are some general types of penetration tests that ethical hackers perform on a regular basis:

### WEB APPLICATION TESTING

Web application testing tests software accessed through the internet. Assessments such as SQL injections can determine whether an organization's web-based programs have scripts that criminals can manipulate. Web applications can be exposed on the server or client side so thorough testing is needed to protect data.

### MOBILE APP TESTING

There could be security issues with the design of the app that enable hackers to break into a company's network. With mobile app testing, ethical hackers can use different techniques to find bugs or other holes in authentication or password encryption.

### SOCIAL ENGINEERING TESTING

Social engineering testing determines the vulnerability of an organization's employees. Shred-It's state of the industry report in 2018 found that 47 percent of C-suite executives identified human errors by employees as the cause of data breaches. To test susceptibility to attacks, ethical hackers may send out spear-phishing emails and determine the response rate from employees.

## WIRELESS TECHNOLOGY TESTING

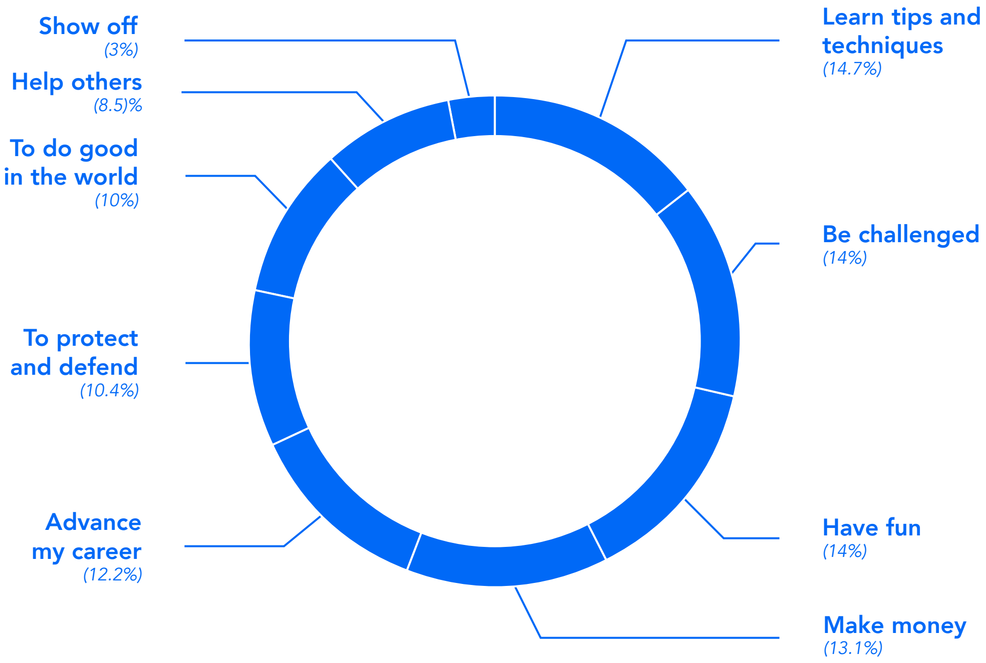
An unsecure wireless setup can be easily compromised. Wireless technology testing determines how secure a wireless network is. A wireless pen test might also try to exploit how a company's employees are using software on their devices to help find weaknesses.

## WHAT MOTIVATES ETHICAL HACKERS

In its latest report, security company HackerOne found a variety of motivations for why its individuals hack. Surprisingly, money was not the primary reason hackers exploit vulnerabilities. Instead personal reasons polled the highest.

The most common answer to "Why do you hack?" was to learn techniques and improve hacking skills. At the same time, profit motivations fell to fourth place from the first place in 2016. Overall, most ethical hackers want to challenge themselves, have fun, and learn while probing for cybersecurity weaknesses.

## WHY DO YOU HACK? TO . . .



Source: https://www.hackerone.com/sites/default/files/2018-01/2018_Hacker_Report.pdf

# IS HACKING LEGAL?

Sometimes. Hacking like that of white hat hackers, which requires authorization from an organization to test its cybersecurity, is legal and necessary for protection. Hacking for personal or financial gain, fun, or to make a political statement is illegal, though.

In fact, unethical hacking is an activity the United States legal system takes seriously. According to the National Conference of State Legislators, all 50 states have laws regarding computer crimes, and some directly address unauthorized access and criminal hacking. In addition, U.S. Congress passed the Computer Fraud and Abuse Act in 1984 to address computer crimes in federal jurisdiction.

Furthermore, even though the practice of ethical hacking is allowed, there are still some potential legal issues that can come up. According to an article from ZD Net, some companies do not have clear channels for hackers to communicate vulnerability reports. When some companies find out they have a vulnerability, they can become upset and threaten legal action, even if the hacker's intentions were good.

When participating in ethical hacking, it's important to be sure that an easy-to-understand contract has been put in place so both sides feel safe about testing for weaknesses in their systems. Both ethical hackers and the organizations they work with need to understand the scope of the hacking and what will be communicated back to the company.

# WHAT YOU NEED TO BECOME A WHITE HAT HACKER

In order to become an ethical hacker, you'll first need to learn some key computer skills. This starts with understanding programming languages, such as:

- **C:** Used in standard operating systems like Windows
- **C++:** Used by Adobe Suite and Facebook
- **JAVA:** Used in Android phones and in Big Data companies
- **PYTHON:** Used in websites like Google, Yahoo, and Spotify

You can boost your credentials as a cybersecurity professional by pursuing a certificate in ethical hacking (CEH). Many organizations offer these certifications to people once they have begun their professional career. A certification shows employers that you are a trusted hacker, and you have proven to have a high level of technical skill.

# CAREER OUTLOOK

A report from the Herjavec Group and Cybersecurity Ventures has estimated there will be upwards of 3.5 million cybersecurity jobs available in 2021, with a large amount going unfilled. If you want to work as a white hat hacker, there are multiple job avenues you can pursue depending on your interests and goals. Salary figures are provided by PayScale.

## INFORMATION SECURITY ANALYST

***Median Annual Salary: $70,450***

Information security analysts produce solutions to patch up the cracks in a company's cyber defenses and carefully document any breaches that take place. These analysts also conduct research, test an organization's technology infrastructure, coordinate technology updates throughout an organization, and manage security principles based on privacy policies and data.

## PENETRATION TESTER

***Median Annual Salary: $81,076***

Penetration testers conduct evaluations and test to discover what security vulnerabilities exist within a company's cybersecurity, networks, or software. Penetration testers also seek out and address passive threats to network integrity, such as poor password policies and user security practices. Many penetration testers may create their own tests based on the needs of companies.

## CHIEF INFORMATION SECURITY OFFICER (CISO)

***Median Annual Salary: $156,663***

A career to strive for, CISOs are in charge of an organization's cybersecurity strategy and department. They lead a team of cybersecurity professionals and evaluate and suggest new ideas to face any existing or potential threats to the security of an organization's data. As cybersecurity leaders, much responsibility falls on CISOs to keep companies safe from breaches.

# YOUR FUTURE AS AN ETHICAL HACKER

As technology continues to change and improve, organizations will need people like you to protect their valuable assets. Cybersecurity professionals are the heroes of our cyber lives and make a tremendous difference in keeping individuals' and organizations' data safe.

If you're interested in making a difference in cybersecurity, consider a career in information technology. The most efficient way to start on the path to becoming an ethical hacker is with an online bachelor's degree. At King University, you can earn an online IT degree quickly and start impacting the field of cybersecurity. Our degree program has four tracks to allow you to focus your studies on a specific branch of information technology.

- **CYBERSECURITY MANAGEMENT:** Take a deep dive into cybersecurity with courses about cybersecurity policy, cybersecurity forensics, and the cybersecurity of mobile devices.

- **CLOUD COMPUTING AND SYSTEMS ADMINISTRATION:** Go in-depth as you learn about wireless and mobile network managements as well as implementing enterprise and wide area networks.

- **INFORMATION SYSTEMS:** Gain knowledge from both cybersecurity and network management courses that will prepare you for a career in information technology and security.

- **DIGITAL BUSINESS AND GAME DEVELOPMENT:** Learn the planning and development of domain-specific and work-related games, digital media, and training production for a variety of businesses and enterprises.

King University has been nationally recognized for its programs by U.S. News & World Report, The Princeton Review, and the Brookings Institution. With affordable tuition, a generous transfer policy, and year-round classes, we help you balance your educational aspirations with your busy life. Our accelerated online courses are designed so you can complete your degree and start your career quickly.

KING
UNIVERSITY
ESTABLISHED IN 1867