WEBROOT®

an opentext™ company

WHY HACKERS HACK

It's Your Business to Care!

Webroot.com/LockdownLessons

LOCKDOWN LESSONS

INTRODUCTION

As cybersecurity grows more complex, criminals around the world are evolving along with it. Their methods leave you vulnerable and many organizations are at risk. Staying informed on this ever-changing landscape is vital. In this educational eBook, we explore the minds of hackers and open the window into their world. Learn why it's important to debunk the common stereotypes, get informed on their methods and motives, and find out who they target the most. IT security experts Tyler Moffitt, Kelvin Murray, and Grayson Milbourne offer help as you navigate today's uncertain waters and lend tips on how to lock down your business and protect your customers from ongoing threats.

WEBROOT®
an opentext company

THE STEREOTYPE

When you think of a hacker, do you envision an anti-social, young hoodie-wearing man in a dark basement? Popularized by Hollywood and mainstream media, this is the image many of us see, although it's not entirely accurate. These stereotypes teach us to think of hackers only as nefarious individuals who will stop at nothing to wreak unstoppable havoc. However, the reality is that hacking is a variable, diverse, and highly indvidualized practice, and not all hackers are cybercriminals. In fact, some hackers can even help strengthen your digital defenses!

The History of the Hollywood Hacker

The modern portrait of a hacker has been forged by popular films and television shows that perpetuate the myth of the young, reckless computer genius who can hack anything. The origins of this stereotype actually begin as early as the 1960s, with British comedy caper, *The Italian Job*. Thanks to the film's success, the stereotype continued to evolve over the following decades until a more accurate portrayal appeared in 2015.

The Italian Job (1969)

A robber gets help from a group of Britain's most infamous computer hackers to steal gold bullion. This was one of the first Hollywood depictions of hacking as a glamorous and profitable trade.

WarGames (1983)

A high school student hacks into a military computer and accidentally activates the U.S. nuclear arsenal. One of the earliest films to envision the devastating global consequences of a single cyberattack.

Hackers (1995)

A teenage hacking group must prove that a sinister superhacker is framing them for embezzlement. Famously one of the first portrayals of a female hacker, played by Angelina Jolie.

The Matrix (1999)

A computer hacker discovers that all life on earth may be nothing more than an elaborate façade. This film helped popularize the fast-hacking "computer genius" stereotype we know today.

Mr. Robot (2015)

A young programmer works as a cybersecurity engineer by day and a vigilante hacker by night. Considered to be one of the most accurate fictional portrayals of real-life hackers.

FACT VS. FICTION

Hollywood often portrays hackers as either righteous vigilantes or evil terrorists. This is a common misconception that romanticizes hacking while ignoring the real dangers; however, accurate depictions can also cause real-world problems. For example, after WarGames premiered in 1983, the U.S. government signed the Computer Fraud and Abuse Act to dissuade hackers from replicating attacks from the film.

While filmmakers and actors take liberties with their depictions, the "Hollywood Hacker" stereotype offers a small glimpse into the real motivations of hackers, like espionage, theft, disruption, and even altruism.

Debunking the Hacker Stereotypes

Hackers wear many hats and have diverse means and motives. One of the biggest hacker myths is that most hackers are computer geniuses, when in reality many hackers utilize lowcode software to write viruses or break into systems with little to no programming knowledge. In actuality, not all hackers are out to ruin your business. Hacker motivations vary, from disruption to financial gain or just for the fun of it.

MYTH	TRUTH
All hackers are "bad guys" out to steal information.	Computer hackers are individuals who use computers, networking, or other technology and skills to gain access to computer systems for different reasons.
All hackers are male.	The average hacker is a male under age 35[1] but hackers can be any age, gender, or ethnicity.
All hackers are lone wolves.	Hackers are coordinated and work within a broad and complex network. They often have salaries, set holidays, bonus payments and sales arrangements that include reseller portals and component rental. It's common for hackers to be involved in larger groups or organizations.
Hackers have to work fast.	Hackers usually aren't concerned with a ticking clock, and many take a slow and methodical approach to get what they want.
There's very little money in hacking.	The average cost of a data breach is $3.92 million,[2] and 71% of breaches are financially motivated. The average hacker can earn up to 40 times the median wage of a software engineer.[3]
Hackers only attack large corporations.	SMBs are prime targets. More than 70% of cyberattacks target small businesses[4] and MSPs hold the keys when it comes to data access.

DID YOU KNOW?

Cybercriminals use automation to do the work of a full team of hackers! AI-based cyberattacks can strike multiple businesses at once, and no business is too big or too small to be a target.

By better understanding the true methods and motivations behind the myths, you can learn how to protect your business and customers against today's biggest threats.

1, 3 HackerOne. "The 2019 Hacker Report." (August 2019)
2 Security Intelligence. "2019 Cost of a Data Breach Report." (July 2019)
4 Verizon. "2019 Data Breach Investigations Report." (May 2019)

THE PROFILE

Hackers typically fall into three distinct categories: black hat, white hat, and grey hat. Black hats are hackers who violate computer security for malicious intent, while white hats test existing internet infrastructures to find loopholes or bugs in the system, typically to improve security. Grey hats fall somewhere in between, often breaking into systems illegally but without malicious intent. There are also many subtypes of black, white, and grey hat hackers with various means and motives, from the novice script kiddie to the nation-state terrorist.

Black, White, and Grey Hat Hackers

Why do we categorize hackers by their "hats"? The analogy harkens back to the U.S. westerns of the 1930s and 40s, when the good guys wore white cowboy hats and the villains donned black ones. While this is an oversimplification, the hat archetype helps us define different groups of hackers based on their behavior and motivations.

Black Hats

Also known as cybercriminals or threat actors, black hat hackers violate computer security with malicious intent or for personal gain. Talented black hats not only profit from targeting businesses and individuals, but also from selling their tools to less technically capable hackers ("script kiddies"), such as ransomware-as-a-service or exploit kits for hire. Black hats are generally highly skilled, but don't underestimate beginners. They can easily strike a big target with the right tools.

White Hats

Also known as ethical hackers, white hats work to test existing internet infrastructure to research loopholes or find bugs in a system. White hats have historically been pivotal in ensuring that organizations maintain a secure network. They often work as employees or consultants, usually for governments and large corporations, although some partner with MSPs and security companies to help SMBs. There are at least 300,000+ registered white hat hackers around the world.[5]

Grey Hats

Grey hat hackers are those whose hacking practices may violate ethical standards but are generally performed without malicious intent. Similar to white hats, grey hats often hack into computer systems to notify the administrator or owner that their network contains vulnerabilities, which must be fixed. However, unlike white hats, grey hat hackers may not work for an official company and can choose to extort victims, offering to remove bugs for a nominal fee.

WHY DO THEY HACK?

Financial gain is a primary driver for black hat hackers, and hacking can be highly profitable. Black hats generally earn money through theft, fraud, extortion, and other nefarious means.

White hat motivations vary, although money and altruism top the list. The average Certified Ethical Hacker earns around $91,000 per year.[6] "Bug bounties" are one way for white hats to legally profit and gain recognition.

Grey hats may be less malicious than their black hat counterparts, but money is still a major motivator, although some hack for fun or to improve their programming skills.

5 Security Intelligence. "2019 Cost of a Data Breach Report." (July 2019)
6 PayScale. "Certified Ethical Hacker (CEH) Salary Data." (December 2019)

Hacker Subtypes

Between the most altruistically motivated white hat to the deeply sinister black hat, there is a wide range of hacker personas, each guided by the intentions behind their hacking. Understanding the hacker subtypes can help you identify potential threats as well as opportunities to leverage hacking to protect your business.

Script Kiddies

Most commonly associated with the "hacker in a hoodie" stereotype, Script Kiddies are programming novices who have some coding knowledge but lack expertise. They typically use free and open source software, easily found on the dark web, to infiltrate networks, and can be black, white, or grey hat.

Hacktivists

Hacktivists are grey hat hackers with the primary goal of bringing public attention to a political or social matter through disruption. Two of the most common hacktivist strategies are stealing and exposing sensitive information or launching a denial of service (DDoS) attack. One of the most well-known hacktivist groups is Anonymous, infamous for taking down the CIA's website.

Red Hats

Red hats are whiter shade of grey hats whose sole objective is to block or destroy the efforts of black hat hackers. Considered the "vigilantes" of the hacker world, red hats will attempt to shut down malicious attacks with their own tools rather than reporting the breach.

Nation-State

Nation-state hackers are those who engage in espionage, social engineering, or computer intrusion with the goal of acquiring classified information or seeking large ransoms. Backed by governments, they are often sophisticated and well trained.

Malicious Insiders

An insider may be a disgruntled current or former employee who steals or destroys information, or someone hired by a competitor to pilfer trade secrets. The most valuable data for a malicious insider is usernames and passwords, which can then be sold on the dark web to turn a hefty profit.

> **"While this didn't used to be the case years ago, most black hats now are hacking for monetary gain because there's so much money to be made in hacking. Even white hats who use their powers for good can make a profit."**
>
> — Tyler Moffitt, Senior Threat Research Analyst, Webroot

Hackers can target any business for any reason! Understanding their methods and motivations can help you keep your business and your customers safe.

BEHIND THE HOODIE

Most social stereotypes are easily debunked, and hoodie-clad hackers are no exception. The average hacker comes in all shapes and sizes—often disguised as the boy or girl next door. Targets of cybercrime are equally diverse. Many hackers will seek out low-hanging fruit, and the biggest vulnerabilities are often the result of human error. Weak passwords, lax email security, and out-of-date technologies are all easy wins for hackers, and no business or industry is truly safe. In fact, hackers can specialize in breaching specific business types or industries, such as healthcare or finance, refining their expertise with each new attack.

Who They Breach: The Tricks of the Trade

Along the same lines as today's hoodie stereotype, small and medium-sized businesses hold a dangerous misconception that hackers only target large organizations, when in fact any business that handles personally identifiable information (PII), bank accounts, health data, and other sensitive information are vulnerable. The simple truth is, the majority of criminal money is being made from SMBs in key verticals. So who is a target?

Managed Service Providers

MSPs hold plenty of valuable data for multiple customers across industries, which makes them prime targets. Island hopping is a common hacking technique wherein hackers jump from one business to another via stolen login credentials. MSPs and their SMB customers are both potential targets of these attacks.

Healthcare Organizations

Hospitals, physical therapy offices, pediatricians, chiropractors, and other healthcare practices are easy targets for cybercrime due to their chaotic and sometimes lax security practices. Medical data and research is highly valuable to the right buyer. On the dark web, patient records alone can sell for up to $1,000 or more.[7]

Municipalities, Infrastructure, and Utilities

Cities can also fall victim to cyber attacks. Not only is the massive amount of data stored in city systems attractive, hackers can also launch disruptive ransomware attacks, shutting down infrastructures or utilities until they get paid. Many cities still rely on out-of-date legacy systems that are vulnerable to malware or ransomware.

Government Agencies

Local and national governments are primary targets for cybercriminals, particularly nation-state terrorists, for a variety of reasons. Small governments and local agencies generate troves of sensitive information, while large governments can be victims of nation-wide disruption.

Financial Institutions

Banks, credit unions, and other financial institutions have long been targets for hackers due to a wealth of data and money. In fact, in 2018, over 25% of all malware attacks targeted banks—more than any other industry.[8] What's more, automation has further enabled cybercriminals to run advanced attacks on financial institutions at scale.

Celebrities, Politicians, and High Profile Brands

Hacktivists, who are politically, economically, or socially-motivated, seek out celebrities, politicians, and other prominent organizations as targets. They may even attempt to embarrass public figures or businesses by stealing and disseminating sensitive, proprietary, or classified data to cause public disruption, or for private financial gain via blackmail.

7 CBS News. "Hackers are stealing millions of medical records – and selling them on the dark web." (February 2019)

8 Forrester. "The Total Economic Impact of the IntSights External Threat Protection Suite." (October 2019)

How To Protect Against Malicious Hackers

The only prerequisite for becoming a target is having something that hackers want, which puts all businesses at risk. Luckily, threat awareness and a proactive approach to security can go a long way in keeping your business secure. While hackers have diverse means and motives, for black hats and other malicious meddlers your business holds the keys to the kingdom. It's up to you to know their methods and to protect your business and your customers from advanced threats.

Think Like a Hacker

Security awareness is a vital component of effective cybersecurity. In fact, Webroot's own research found that security awareness training cut clicks on phishing links by 70%[9] when delivered with regularity. Understanding hacker practices and motivations can help you predict potential threats and thwart attacks more effectively.

Lock Down Your Business First

The right security layers can protect you from threats on all sides. Check out more of Webroot's free educational videos, podcasts, and cybersecurity guides in our **Lockdown Lessons Resource Center** to discover how layered cybersecurity can benefit your business.

Leverage Automated Threat Detection

As modern attacks continue to increase in complexity and as attacks are automated at scale, your business will become more targeted. The best way to combat targeted attacks is to quickly and automatically remediate threats that do get through. Automated Detection and Response (ADR) solutions improve the accuracy of detection and speed of response, which are critical against attacks.

Protect Your Customers

Your customers may be underequipped to handle a breach. MSPs are in a unique position to offer high-quality, comprehensive security awareness training as well as cybersecurity expertise and automated protection for SMB customers. SMBs looking to strengthen their security posture should also look to partner with MSPs and other managed security providers to secure their own networks and systems.

> **"One of the biggest trends we've seen over the last few years has been the specialization of criminal hackers."**
>
> — Kelvin Murray, Senior Threat Researcher, Webroot

Understanding why hackers are after your business and what methods they use to break into your systems can help you stop attacks before they happen.

9 Webroot. "Webroot 2019 Threat Report." (February 2019)

CONCLUSION

Although hackers are diverse and hacking as a profession is more complex than many realize, the targets of cyberattacks remain consistent: the reality is that every business is a potential target for malicious hacking — including you and your customers! Cyberattacks against MSPs and SMBs are on the rise, making it imperative to protect against all types of threats. Locking down your business starts with being educated about hackers and their methods, but it doesn't stop there. Protect your customers with the most advanced cybersecurity solutions that can help close security gaps and quickly remediate threats.

Don't Wait to Protect Your Business

What you don't know can hurt you! Start a free Webroot trial and see for yourself how our solutions can help you prevent threats and maximize growth.

About Webroot

Webroot, an OpenText company, harnesses the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide endpoint protection, network protection, and security awareness training solutions purpose built for managed service providers and small businesses. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Webroot operates globally across North America, Europe, Australia and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.

Check out our Lockdown Lessons podcast series, guides, and other resources to help MSPs and businesses navigate today's cyber threat landscape and be their most successful.

Visit webroot.com/LockdownLessons

LOCKDOWN LESSONS