LOCKDOWN LESSONS

WEBROOT®
an opentext™ company

Why Hackers Hack: 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 Weak passwords, lax email security, and out-of-date technologies are all easy wins for hackers, and no business or industry is truly safe.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.[1]

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 Many cities still rely on out-of-date legacy systems that are vulnerable to malware or ransomware.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 nationwide 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.[2] 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.

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

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

> “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.

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.

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.

Think Like a Hacker

Security awareness is a vital component of effective cybersecurity. In fact, Webroot’s own research found that security awareness training reduced clicks on phishing links by 70%[3] when delivered with regularity. Understanding hacker practices and motivations can help you predict potential threats and thwart attacks.

Lock Down Your Business First

The right security layers can protect you from threats on all sides. Check out 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 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 SMB customers high-quality, comprehensive security awareness training along with cybersecurity expertise and automated protection. 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.

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.

Don’t wait to protect your business!

What you don’t know can hurt you! Cyberattacks against MSPs and SMBs are on the rise. Start a free Webroot trial and see for yourself how our solutions can help you prevent threats and maximize growth.

Start My Free Trial

[3] Webroot. “Webroot 2019 Threat Report.” (February 2019)