WHY DO HACKERS HACK?

KYBER SECURITY

The Average Hacker

Most social stereotypes are easily debunked, and hoodie-clad hackers are no exception. The average hacker comes in all shapes and sizes and are often disguised as the boy or girl next door.

Targets of cyber crime 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 Weak passwords, lax email security, and out-of-date technologies are all easy wins for hackers, and no business or industry is truly safe.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.

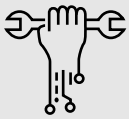
Sales@KyberSecure.com

(203) 333-4444

www.kybersecure.com

Who They Target

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 personal 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 are they targeting?



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. It is important to partner with a MSP that has cyber security at the top of mind.

Healthcare Organizations

Healthcare practices are easy targets for cyber crime 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]

Nonprofit Organizations

Nonprofit organizations collect incredibly sensitive information about their members and donors, which can include social security numbers, credit card information, and even medical information. Without proper measures in place, one single breach could end an entire organization and its mission. Many nonprofts still rely on out-of-date legacy systems that are especially vulnerable to malware or ransomware.

Government Contractors

Department of Defense (DoD) contractors are suspectible to targeted cyber attacks and nation-state terrorists. Such breaches hold critical risk as the data they carry could potentially expose intellectual property pertaining to weapons, materials, and R&D that could compromise military and defense readiness.

Financial Institutions

Financial institutions have long been targets for hackers due to a wealth of data and money. Breaches in the Financial sector exposed 61% of the total sensitive records in 2019 - the highest of any other industry.[2] What's more, automation has further enabled cyber criminals to run advanced attacks on financial institutions at scale.

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

2 Identity Theft Resource Center. "2019 End of Year Data Breach Report." (January 2020)

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 Kyber Security

Our mission is to ensure that your organization has cyber security at the top of mind. To achieve this mindset, we utilize a defense in depth approach with a combination of traditional technologies and new technologies. As the cyber threat landscape constantly evolves, your security measures should be one step ahead.

Kyber Security has dedicated professionals experienced in protecting your organization from ever increasing cyber threats. We are a team who understands that managed security and support services are a vital piece of your company's overall survival. You get a team that is well-versed in IT support and puts security above all else. We will work tirelessly to keep your company protected from the next big cyber attack.

Sales@KyberSecure.com

(203) 333-4444

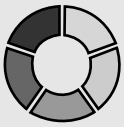
www.kybersecure.com

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, research shows that security awareness training can reduce 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.



Follow A Framework

A framework such as the cybersecurity framework created by the US National Institute of Standards and Technology (NIST) was built with the intentions of allowing organizations to measure their cybersecurity posture relative to the threats they face. By aligning your people, processes and technology with a framework, you can create a seamless cybersecurity program and culture.

Leverage Advanced Technology

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. Advanced monitoring solutions improve the accuracy of detection and speed of response, which are critical against attacks.

Implement Multiple Layers of Defense

Today's standard security solutions are no match for sophisticated attacks, as hackers continue to develop more unique ways to penetrate organizations. Reducing the risk of infections requires a multi-layered approach, rather than a single product.

It's up to you to know hacker methods so you can protect your business. Your cyber risk rating can help establish a plan to defend against critical attacks to your organization. Our Cyber Risk Gap Analysis assessment will help you make the best informed decision on the security improvements or changes needed within your organization. Simply visit the link listed below to learn more.

kybersecure.com/nist-csf-gap-analysis

KYBER SECURITY

[3] Webroot. "Webroot 2019 Threat Report" (February 2019)