SecurityAwarenessNews

the security awareness newsletter for security aware people

The Cybercrime Issue

5 Biggest Threats to Security

Everything You Need to Know About Cybercrime

How You Can Take a Byte Out of Cybercrime

EVERYTHING YOU NEED TO KNOW ABOUT CYBERCRIME

WHAT IS IT?

Cybercrime is typically defined as **the use of computers and other network-connected devices to perform illegal activities**. A few examples: phishing attacks, identity theft, data theft, and cyber extortion (such as ransomware, which encrypts your data until you pay a ransom).

HOW COMMON IS IT?

A quick internet search of "cybercrime statistics" yields all kinds of scary stats like "there is a cyberattack every 39 seconds" or "one in five people will have their credit card information stolen this year," and so on. While statistics can sometimes be misleading, there's no doubt that **cybercrime is a massive industry that continues to grow each year**.

HOW MUCH DAMAGE CAN IT CAUSE?

Like most crimes, **money rules everything**. Cybercrime can place unimaginable financial burdens on organizations in all industries. It can also severely damage an organization's reputation with customers and business associates, sometimes resulting in legal action and eventual layoffs or terminations. Worse yet, when critical resources are attacked—like hospitals or power grids—cybercrime threatens lives.

WHO DOES IT TARGET?

Quite frankly, **cybercrime targets everyone and every organization**. High-profile individuals like celebrities or government officials typically have a lot more to lose than an everyday citizen, so they offer more value to attackers. But cybercriminals will be happy to also target you and attempt to gain access to your bank account or confidential information.

WHAT CAN YOU DO ABOUT IT?

Stopping cybercrime doesn't require a cape or superpowers. Instead, **it requires strong human firewalls who think before they click, use common sense, and always follow policy.** Keep in mind that while some cybercriminals use sophisticated methods to break through cyberdefenses, most cybercrime is carried out by targeting humans wherever possible. So when you're at work, out and about, or at home, keep your eyes and ears open, and help make the world a safer place.

5 BIGGEST THREATS TO SECURITY

SOCIAL ENGINEERING

Social engineering is the art of manipulating, influencing, and deceiving humans for nefarious purposes. Social engineers attempt to hack your emotions to convince you to perform a risky action like clicking on a phishing link or releasing sensitive information over the phone. These attacks lay the foundation for most scams and are often the root cause of security incidents.

RANSOMWARE

Usually spread via phishing attacks, ransomware encrypts computers or data until the victim pays a ransom to gain the decryption keys (or manages to restore systems with unaffected backups). This attack represents one of the most pervasive and dangerous forms of cybercrime, sometimes putting lives at risk (when it hits hospitals) or severely disrupting society (when it compromises entire cities or municipal services).

PHISHING

Phishing is the default strategy in a cybercriminal's playbook. Many phishing attempts feature common red flags, such as grammatical errors or a sense of urgency, but others are much more sophisticated (such as CEO fraud, in which the attacker pretends to be your boss and asks you to wire money). Phishers also target you via text messaging (known as smishing) and real-life phone calls (known as vishing).

UNPATCHED VULNERABILITIES

Out-of-date systems and devices leave backdoors open for cybercriminals. It's one of the few ways they can gain unauthorized access with minimal human interaction (such as someone clicking on a malicious link or downloading an attachment). By enabling automatic updates, you effectively close those doors and improve security.

INSIDER THREATS

The unfortunate reality about security is that while most attacks come from outside of the organization (as in, from criminal hackers), most security threats come from inside the organization. If you have access to our systems, networks, and confidential data, you are a threat to that access. Security breaches are made possible by human error—clicking on a phishing link, accidentally sending data to the wrong party, not following policy, and so on. That's why we focus on common sense awareness and hope to build a culture of resilient human firewalls who prioritize security in everything they do.

HOW YOU CAN TAKE A BYTE OUT OF CYBERCRIME

As in, a byte of data. Get it? Because we're talking about cybercrime and digital safety...

Anyway, thwarting cybercriminals isn't an overly complicated process. Let's break down how you can prevent cybercrime in three important phases of life: at work, at home, and on the go.

PREVENTING CYBERCRIME AT WORK

Let's start with the easy part: **don't fall for phishing attacks.** You can spot them by searching for common red flags such as poor grammar and terrible spelling, a sense of urgency, a call to click on or download something, threatening language, and unrealistic promises.

Of course, not every phishing attack will exhibit those red flags. So double-check the "from" address. Hover over links to reveal the full URL. Remain skeptical of any requests for sensitive data or money. When in doubt, don't click, don't respond, don't download anything. If it appears to come from someone you know, contact that person, and confirm they sent the message.

Phishing aside, keep your work area organized and lock your workstation when not in use. Be sure to close doors behind you. Never allow someone to borrow your credentials to log into a system or enter a secured area. Always follow policy. And report security incidents immediately.

PREVENTING CYBERCRIME AT HOME

Let's start with the easy part: don't fall for phishing attacks (see above).
Next, we recommend developing a security policy for your household, similar to what most organizations enforce. Here are a few security action items to apply to your personal life:

- *Protect every account and every device (including your router) with a strong, unique password.*
- *Enable automatic updates wherever possible.*
- *Set social media accounts to fully private and only "friend" people you know.*
- *Limit what you share on the internet.*
- *Set up different user accounts on shared devices and limit administrator access.*
- *If you have young children, consider using parental monitoring software.*

PREVENTING CYBERCRIME ON MOBILE

When you're out and about, never connect to a public network without using a virtual private network (VPN), which encrypts your connection and prevents data theft. Even when using a VPN, avoid logging into accounts that contain highly sensitive data.

Before downloading any apps or software, research the developers, and only install from trustworthy sources. App stores are frequently targeted by cybercriminals who attempt to spread malicious apps that often impersonate legitimate versions.

Keep an eye on your devices, and never leave them unattended. Consider enabling "find my device" services if available. These allow you to locate your phone via a second device or remotely reset it to factory default (removing all personal information).