Cybersecurity Awareness: It's not just for IT!

10 Tools and Topics Everyone Should Know

Against an ever-expanding attack surface, cybercriminals continue to evolve their tactics, techniques, and procedures (TTP) to execute any manner of attacks. Given the vast array of interconnected devices and networks, it's not difficult to imagine the risk to data and systems as threat actors seek out gaps in an organisation's defence in-depth. While terms like malware, phishing, and dark web may seem like an IT security problem, they're part of the reality of everyone's life in today's workplace. The more we communicate, work, and share information within an "always-on" environment, it's essential all members of an organisation understand some cybersecurity basics to better protect critical assets. To help in this effort, here are 10 cybersecurity tools and topics for becoming more cybersecurity aware.

1 Business Email Compromise (BEC)

A form of phishing, business email compromise (BEC) typically occurs when a threat actor poses as a legitimate business colleague—such as a coworker, vendor, or partner—to facilitate malicious activity. Perpetrators of BEC may be trying to gain payment (such as convincing employees to send them money), exfiltrate data, or otherwise harm the business for their own gain.

2 Dark Web

Many people first heard of the "dark web" via the Silk Road scandal in the mid-2000s and the site's eventual shutdown in 2013. However, the dark web is more extensive and complex than many realise. Broadly speaking, the dark web is an entire secret Internet that cannot be found via normal routes, such as search engines. It operates beneath the surface and is usually only accessible via tools like Tor. Criminals often use the dark web to conduct business. This is where stolen credentials, Social Security numbers, personal data, hacking tools, and other illegal information is bought and sold by cybercriminals

3 Endpoint Protection (EPP)

Endpoint protection (EPP) is a term encompassing multiple technologies and/or processes that secure an organisation's endpoints (e.g., servers, laptops and desktops, and mobile devices) and protects them against viruses, malware, and other threats. Antivirus or anti-malware software, for example, can be included in endpoint protection.

4 Insider Threat

While many people may think of "hackers" as synonymous with cybersecurity threats, organisations are also at risk from the inside. Insiders are users who have typically been granted legitimate access, such as employees, partners, vendors, or anyone else the organisation allowed access into corporate systems. Whether through mistakes (such as clicking a phishing email) or bad intentions (e.g., stealing data to sell externally), insiders can trigger cybersecurity incidents, such as data leaks. Data prevention programs work to limit the risk of accidental or intentional data loss.

5 Malware

Malware is malicious software that infects users' computers or devices to take advantage of their data. Once the user's computer is infected, the malware can inflict severe damage, such as stealing sensitive data, logging keystrokes, and corrupting files. Users are often unaware when malware gets downloaded onto their computer or attacks their website, which is why installing antivirus software and a web application firewall (WAF) is a must for preventing and detecting malware.

6 Managed Detection and Response (MDR)

When cybersecurity threats arise, they need to be dealt with quickly. With a combination of a security operations centre (SOC) and cybersecurity tools, a managed detection and response (MDR) service constantly monitors an organisation's infrastructure, looks for threats, and eliminates them in real time if/when they occur.

7 Phishing

Phishing emails appear in users' inboxes and often appear legitimate but are actually designed to trick people into handing over sensitive information. This often includes payment details such as credit card and bank account information. Always be wary of unexpected emails that ask you to send payment information electronically.

8 Ransomware

Ransomware is a type of malware that's most commonly delivered by email attachment. When a user downloads the attachment, the ransomware gets activated and prevents the user from accessing their systems and data. The user is then informed their data will remain encrypted unless they pay their attackers.

9 Security Operations Centre (SOC)

Defending against cybersecurity threats is a round-the-clock job, and a security operations centre (SOC) is a 24-hour team of experts who proactively hunt for, triage, and respond to threats in real time. Large organisations may have an embedded SOC, but smaller organisations often outsource them

10 Security Information and Event Management (SIEM)

Security information and event management (SIEM) systems are a type of software that companies can use to collect data on activity in their systems and, through correlation of that data, receive alerts for unusual behavior. A SIEM solution generally collects data from across an organisation's systems, analyses it, provides reports, and flags potential threats.

Want to learn more? Contact us today!

Security@trustsystems.co.uk