Digital Security
Progress. Protected.

CYBER HYGIENE:

10 Tips for Sanitizing Your Environment

Cyber Hygiene: 10 Tips for Sanitizing Your Environment

Personal hygiene is a set of habits, daily rituals and actions that keep us safe and healthy. In the same way, practicing cyber hygiene keeps computing resources and data safe and secure. Cyber hygiene practices are, fundamentally, just sound basic security and organizations that don't address cyber hygiene are putting themselves unnecessarily at risk. Many, many cyber attacks take advantage of one or more lapses in basic security to gain a foothold and steal data or plant malware. While preventing that from happening is largely considered the job of security professionals and IT departments, read on and you'll see that everyone in an organization has a role to play.

1. REDUCE THE ATTACK SURFACE

Most companies of medium size or larger have one or more systems that are long-forgotten but still power on because nobody has time to investigate whether they still serve a purpose. Take the time. Look for unused equipment — computers, servers, and devices with embedded systems — that are connected but not being used, and wipe and disable them. Similarly, look for old, unused software and uninstall it. The best practice is to document all devices and software and create an inventory that can be maintained as the environment changes. Automated tools can be helpful here, especially for larger organizations.

2. PROVIDE CYBERSECURITY AWARENESS TRAINING FOR USERS

Today, 74% of all breaches include the human element, including human error, privilege misuse, use of stolen credentials or social engineering. That's why well-educated employees are a critical additional line of defense on top of email and endpoint security solutions. Onboard new employees with comprehensive security awareness training, with annual if not quarterly refreshers for all employees. The program should emphasize how to recognize phishing emails, not clicking on suspicious links and attachments, avoiding public Wi-Fi, safe use of removable drives, and password best practices, among other topics.

3. IMPLEMENT AND ENFORCE PASSWORD HYGIENE

Easily guessed or stolen credentials are one of the most common ways threat actors gain access, and there is a thriving black market for compromised user names and passwords on the dark web. Users who re-use the same password across multiple sites or employ simple, easily guessed passwords make an adversary's job far too easy. Require strong passwords and regular password changes. Establish clear, firm policies regarding password re-use and consider providing password-management software to handle the logins and reduce the temptation.

4. USE MULTI-FACTOR AUTHENTICATION

Requiring MFA is one of the most-effective deterrents against a threat actor attempting to use a compromised password. Current solutions don't overly inconvenience users relative to the strong protection MFA provides; they keep challenges to legitimate users at a minimum while blocking threat actors attempting access from unrecognized devices. MFA is a must for any sort of remote access, including access via VPNs, and is recommended for securing administrative access from any location.

5. EXERT TIGHT CONTROL OVER ADMINISTRATIVE ACCESS

Threat actors aim to gain administrative access so they can make changes at will and then cover their tracks. Don't make it easy for them. Limit the number of users who have administrator privileges and apply the principle of least privilege by granting the minimum amount of permissions necessary to perform the individual job role.

6. KEEP SOFTWARE AND SYSTEMS UPDATED AND PATCHED

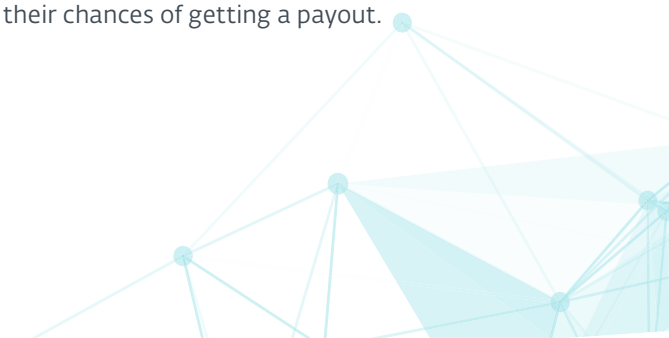
Some of the most notorious, well-publicized and destructive malware attacks could have been avoided by simply applying software patches in a timely manner to close security holes. Since threat actors are quick to exploit newly disclosed vulnerabilities, patching and updating is critical but often falls to the bottom of the task queue when IT has more immediate and pressing matters to attend to. Consider an automated solution that prioritizes and handles much of the workload.

7. BACK UP DATA REGULARLY

Regular backups will greatly assist with recovery from ransomware attacks that encrypt data on computers and servers and attempt to render systems inoperable. The 3-2-1 rule says you should keep three copies at all times, stored on at least two different types of media (tape, disk or in the cloud), and keep one copy offsite. Backups aren't solely about ransomware prevention, either — cyber hygiene is about protecting data so backups are there to restore it in the event of a device failure.

8. PROTECT SENSITIVE DATA WITH ENCRYPTION

Adversaries look for business-critical or personal data they can steal. Most often the motivation is financial — their goal is extortion and they threaten to leak the data by posting it on the dark web unless they receive a payment. If the data is rendered unreadable by encryption, it's useless to them unless they can also get their hands on the encryption key. Note that having backups and encrypting sensitive data to keep it out of the hands of adversaries protects against "double extortion" attacks. Here, threat actors deploy ransomware and threaten to exfiltrate sensitive data to increase their chances of getting a payout.



9. DEPLOY AND PROPERLY CONFIGURE ENDPOINT PROTECTION

Detecting, blocking, and removing malware is often considered the heart of what endpoint protection platforms do, but current solutions have evolved considerably to keep up with threat actors. They use artificial intelligence, behavioral inspection, threat intelligence, and other technologies to keep up with the constantly morphing techniques of imaginative and resourceful adversaries. An endpoint platform that works natively with an extended detection and response (XDR) solution makes the data available for incident investigation, response, and remediation to effectively shut down attacks before they do any real damage.

10. DON'T OVERLOOK CLOUD SECURITY

Use of the cloud for collaboration, often with users who have access from anywhere or with partners from outside the organization, calls for heightened attention to the security risks involved. Establish guardrails around cloud use in areas such as use of unapproved file-transfer services and conditions for third-party access. Ensure that accounts are closed when employees terminate or projects that involve third parties are complete. In addition, a cloud security solution protects against threats being spread via cloud-based email, collaboration platforms or file shares.

About ESET

AI-NATIVE PREVENTION FOR TOMORROW'S THREATS

Stay one step ahead of known and emerging cyber threats with our **AI-native, prevention-first approach**. ESET combines the power of AI and human expertise to make protection easy and effective.

Developed over 30 years, ESET's best-in-class protection is powered by our **in-house global** cyber threat intelligence, including our **extensive R&D network** led by industry-acclaimed researchers.

ESET PROTECT, our scalable, cloud-first XDR cybersecurity platform combines next-gen prevention, detection, and proactive threat hunting capabilities, and a wide range of security services including managed detection and response (MDR). Our highly customizable, integration-ready solutions support all deployment methods, include local support and have minimal impact on performance. They identify and neutralize known and emerging threats before they can be executed, support business continuity, and reduce the cost of implementation and management.

Our mission isn't just to stop attacks in their tracks; it's to prevent them from ever happening. ESET protects your business so you can unlock the full potential of technology.

ESET Digital Security
Progress. Protected.