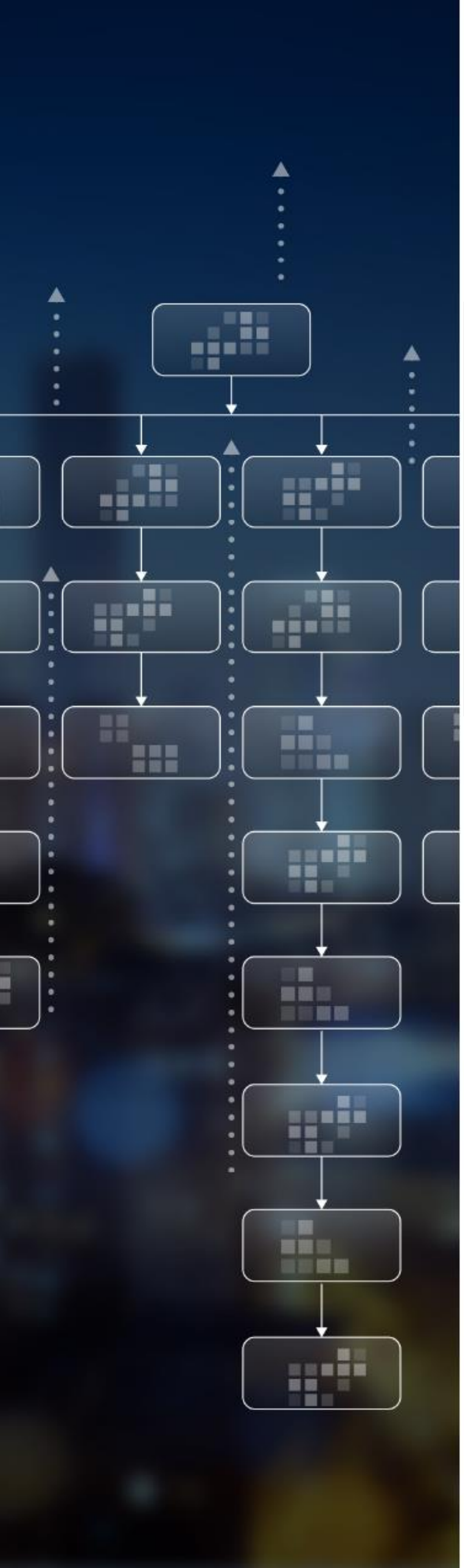


What is Cyber Hygiene and Why is it Important?

TechTarget

In this handbook:

Cyber hygiene, or cybersecurity hygiene, is a set of practices organizations and individuals perform regularly to maintain the health and security of users, devices, networks and data. This guide will walk you through why cyber hygiene is important.

In this handbook:

What is cyber hygiene and why is it important?

ALISSA IREI, SENIOR WRITER

Cyber hygiene, or cybersecurity hygiene, is a set of practices organizations and individuals perform regularly to maintain the health and security of users, devices, networks and data.

The goal of cyber hygiene is to keep sensitive data secure and protect it from theft or attacks. The concept works similarly to personal hygiene. Individuals maintain their health by taking precautionary measures to help ensure it, such as flossing to minimize cavities and handwashing to stop the spread of disease. Organizations can maintain their health and prevent data breaches and other security incidents by following precautionary cyber hygiene measures.

It is important to note that the onus of cyber hygiene is not just on IT security managers, analysts and technicians. Rather, it is a shared responsibility that all departments and users must prioritize. One way almost every employee can help maintain proper cyber hygiene is by following current email security best practices, such as avoiding public Wi-Fi and creating strong, unique passwords.

WHAT ARE THE BENEFITS OF CYBER HYGIENE AND WHY IS IT IMPORTANT?

The benefits of cyber hygiene speak for themselves. By maintaining good cyber hygiene, an organization minimizes the risk of operational interruptions, data compromise and data loss by improving its overall security posture.

An enterprise's security posture refers to the overall strength of its cybersecurity program, and therefore how well it is positioned to handle existing and emerging threats. Basic cyber hygiene goes a long way toward achieving optimal cybersecurity.

Poor cyber hygiene can lead to security incidents, data compromise and data loss. The consequences of a data breach may include financial loss, government fines, operational downtime, organizational upheaval, damage to the organization's reputation and legal liability.

WHAT ARE THE CHALLENGES OF MAINTAINING CYBER HYGIENE?

Maintaining good cyber hygiene is critical but far from easy. Common challenges include the following:

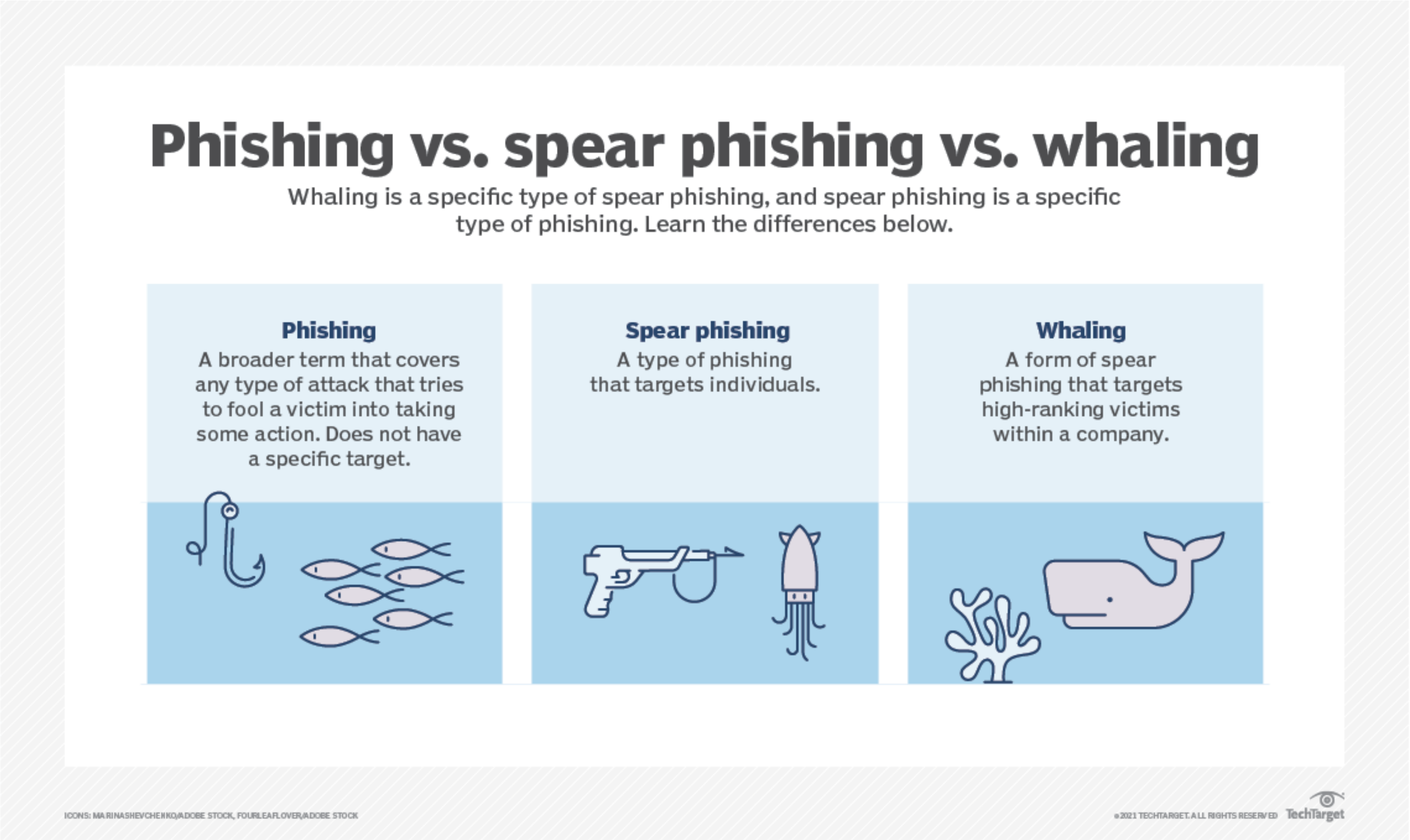
- **The breadth and complexity of IT environments.** In today's enterprise, the sheer volume of users, devices and assets -- often distributed across hybrid and multi-cloud environments -- makes maintaining proper cyber hygiene extremely challenging.
- **Monotony.** As an objective, cyber hygiene can never be completed and crossed off a list. Rather, it requires security practitioners and end users to routinely engage in a never-ending stream of important -- but often mundane and easily neglected -- behaviors and tasks.
- **User buy-in.** IT security teams can't achieve good cyber hygiene on their own. They need the support and engagement of end users throughout their organizations, including those with little expertise or interest in cybersecurity.

CYBER HYGIENE BEST PRACTICES FOR USERS

Cybersecurity is everyone's responsibility, which means that while organizations need to prioritize cyber hygiene, so must individual users.

With that in mind, users need to be aware of the following cyber hygiene best practices:

- **Backups.** Regularly back up important files to a separate, secure location that would remain safe and isolated if the primary network were compromised.



Phishing vs. spear phishing vs. whaling

Whaling is a specific type of spear phishing, and spear phishing is a specific type of phishing. Learn the differences below.

Phishing
A broader term that covers any type of attack that tries to fool a victim into taking some action. Does not have a specific target.

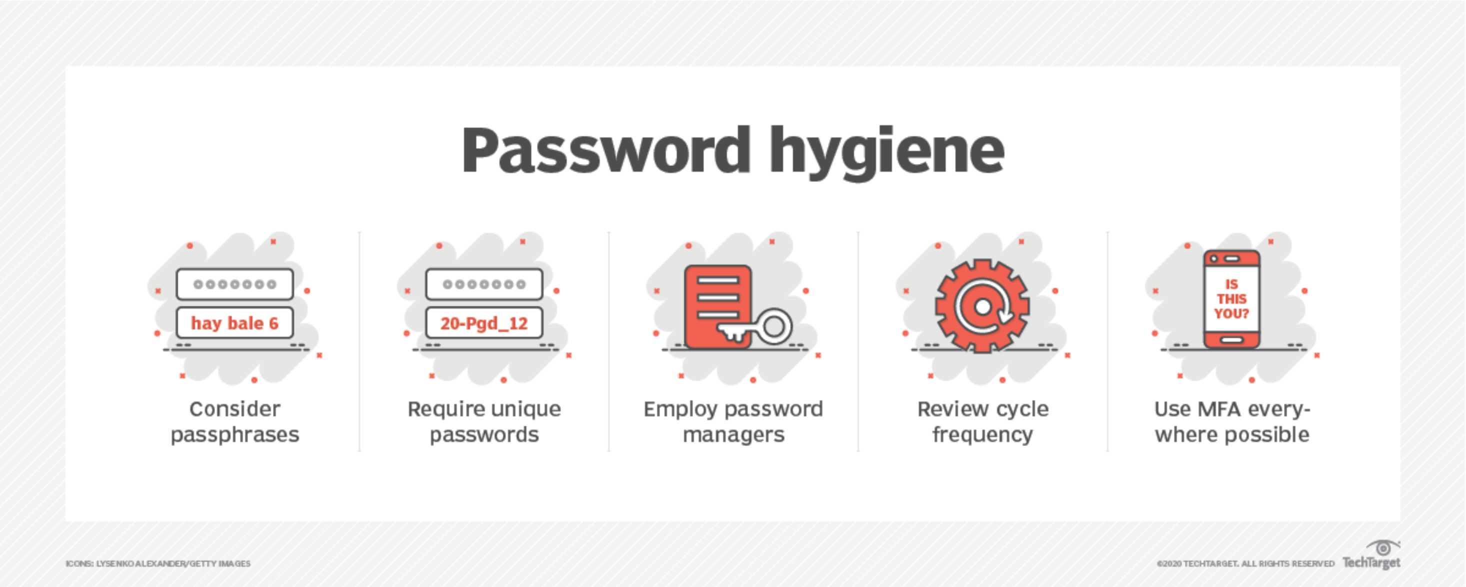
Spear phishing
A type of phishing that targets individuals.

Whaling
A form of spear phishing that targets high-ranking victims within a company.

ICONS: MARINASHEVCHENKO/ADOBE STOCK, FOURLEAFLOVER/ADOBE STOCK

- **Education.** Learn how to avoid getting hooked by phishing scams and how to prevent common malware attacks. As a rule, for example, users should avoid clicking on links and attachments they receive via email. Stay up to date on emerging phishing and malware tactics.

- **Encryption.** Use device and file encryption to protect sensitive data.
- **Firewalls.** Make sure firewalls and routers are properly set up and configured to keep bad actors out of private systems.



ICONS: LYSENKO ALEXANDER/GETTY IMAGES

©2020 TECHTARGET. ALL RIGHTS RESERVED TechTarget

- **Password hygiene.** According to Verizon's 2021 Data Breach Investigations Report, 61% of all breaches involve user credentials. Maintain good password hygiene and use technology such as multifactor authentication (MFA) to make gaining unauthorized access more difficult.
- **Patch management.** Install any available software updates and security patches on both company-owned devices and any personal devices used for work.
- **Online discretion.** Be careful not to post any personal information a bad actor could use to guess or reset a password, or otherwise gain access to private accounts. Be aware of what

personal information is already available online, which cybercriminals could use in social engineering attacks.

- **Security software.** Install security software, such as antimalware and antivirus, to defend systems against malicious software, including viruses, ransomware, spyware, worms, rootkits and Trojans. Make sure the software is properly configured and run regular scans to flag unusual activity.

CYBER HYGIENE BEST PRACTICES FOR ORGANIZATIONS

Achieving optimal personal health and well-being requires an arguably overwhelming array of action items, ranging from flossing to meditating to eating leafy greens to scheduling a colonoscopy. To add to the confusion, recommended practices shift as a person's age and health needs change and as medical science evolves.

Similarly, achieving the best possible security posture can be complex and overwhelming, with a plethora of recommendations and a constantly shifting threat landscape. The right IT security framework and cybersecurity standards can help by offering a starting point for organizing and managing a security program using established processes, policies and practices to set and prioritize cyber hygiene tasks.

An organization looking to improve its security posture might also consult this enterprise cybersecurity hygiene checklist from Ashwin Krishnan, cybersecurity expert and chief diversity amplifier at IT supplier diversity company Mobilematics Inc. Cyber hygiene tools, technologies and action items may include the following:

- **Allowlisting/blocklisting.** Control which applications, websites and email addresses users can and cannot use. Allowlisting -- providing a select list of applications, processes and files users can access -- and blocklisting -- providing a list users cannot access -- are two methods to control access. Learn the benefits and challenges of each approach.

In this handbook:

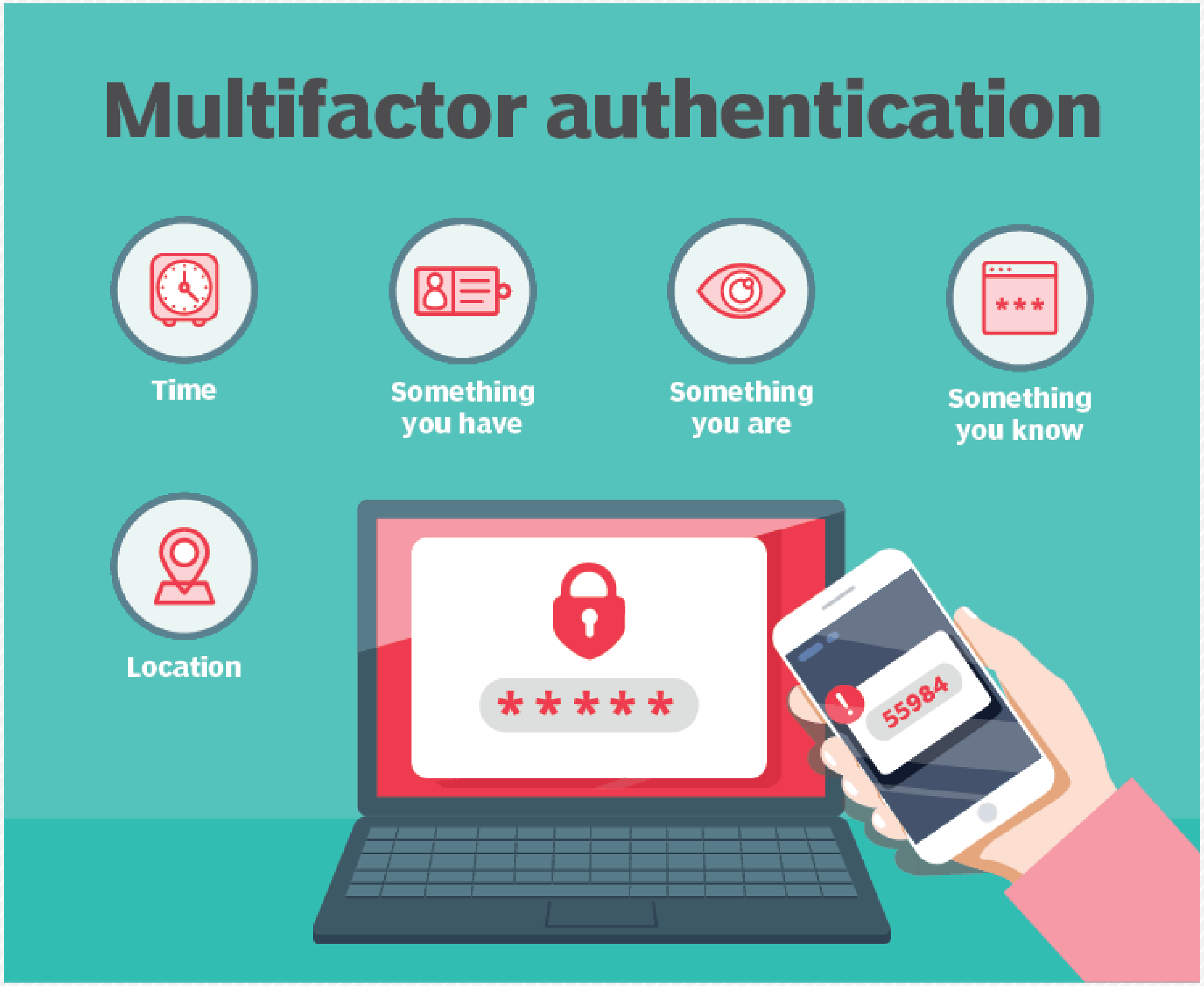


ILLUSTRATION: MYKYTA/ADOBE STOCK, ALEXDNDZ/ADOBE STOCK

- **Authentication and access control.** Authentication, or confirming that a user or device is who or what they claim, is a critical part of cyber hygiene. To secure their networks, organizations can choose from among at least six types of authentication. The most rudimentary is knowledge-based authentication, which requires a user to share preestablished credentials, such as a username and password or PIN. MFA requires two or more authentication factors, such as a password and a one-time code sent to the user's cellphone or email address. Biometric authentication uses biological identifiers, such as fingerprint scanning or facial recognition. Other types of authentication include single sign-on, token-based authentication and certificate-based authentication.

  Security itself hinges on authentication and access control -- the ability to verify and admit certain users while excluding others. Common access control mechanisms include role-based access control, which grants network permissions based on a user's formal position in an organization, and the principle of least privilege, which grants users access to only the assets they absolutely need to do their jobs. Good cyber hygiene requires IT security leaders to periodically review user access entitlement to ensure no one has outdated or inappropriate privileges, which could compromise the overall security posture.

In this handbook:

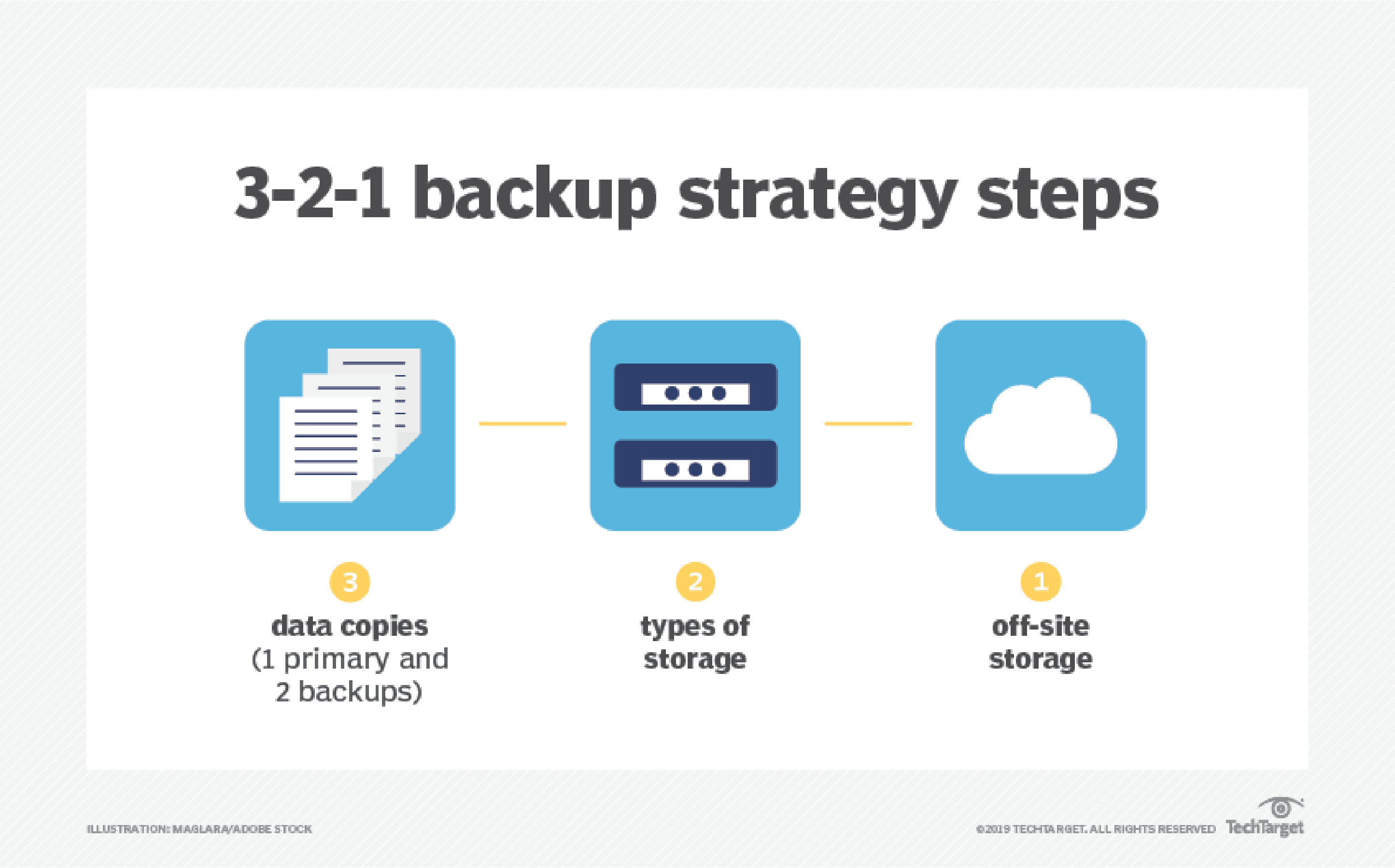


ILLUSTRATION: MAGLARA/ADOBE STOCK

©2019 TECHTARGET. ALL RIGHTS RESERVED TechTarget

- **Backup strategy.** Develop a data backup strategy that ensures mission-critical information is regularly duplicated and stored in a secure location. Many experts recommend following the 3-2-1 rule of backup, which requires storing three copies of data on two different kinds of media -- such as cloud, disk and tape -- and keeping one copy off-site.

- **Cloud access security broker (CASB).** Any organization that relies on IaaS, PaaS or SaaS should consider implementing a CASB as part of its cyber hygiene strategy. CASB software facilitates secure connections between end users and the cloud, enforcing enterprise security policies around authentication, encryption, data loss prevention, logging, alerting, malware detection and more. A CASB gives an organization greater visibility into employee usage of cloud-based applications as well as greater control over the security of cloud-based data.
- **Cybersecurity asset management.** To protect IT assets, one must first know they exist. Enter cybersecurity asset management, a subset of IT asset management (ITAM) that involves discovery, inventory, management and tracking of an organization's assets with the goal of protecting them. That's a tall order for three reasons, according to Nemertes Research CEO Johna Till Johnson:

    1. The staggering volume and variety of IT assets in today's enterprise make it logistically impossible to track them manually via spreadsheets or databases.

    2. Short-lived ephemeral or virtual entities such as virtual machines, microservices and containers mean the corporate attack surface contracts and expands minute to minute.

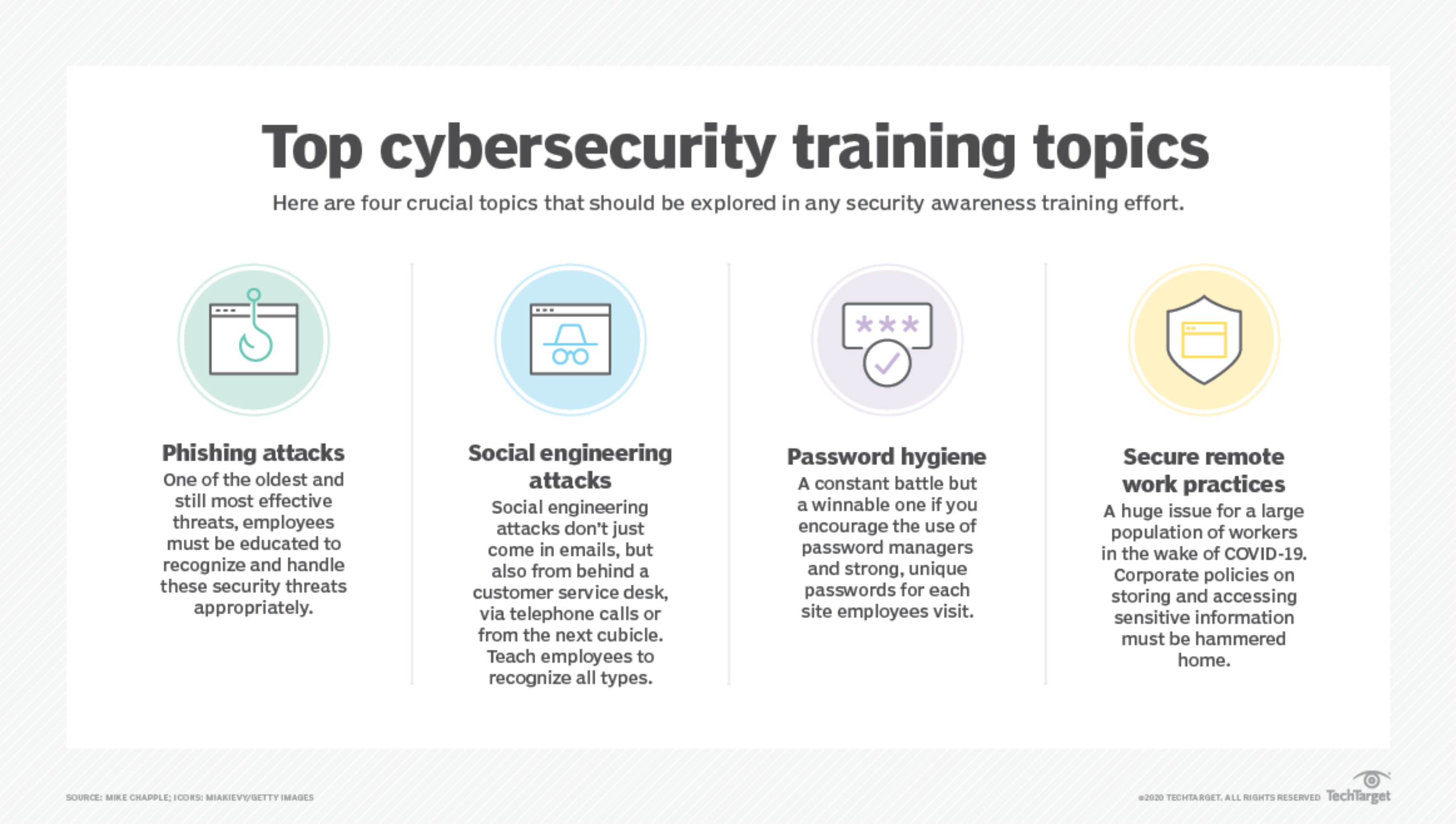
    3. Organizations typically have areas in their environments where ITAM tools don't reach, such as smart facilities with IoT devices.

Despite these challenges, cybersecurity asset management is important and doable, using traditional ITAM tools or more tailored security offerings, Johnson added.

- **Encryption.** Use encryption to ensure the protection of sensitive corporate data, both in transit and at rest.
- **Endpoint security.** In today's workplace, a plethora of endpoint devices operate beyond the traditional security perimeter, putting them and the enterprise network at heightened risk of attack. Identify, manage and secure devices ranging from PCs to IoT nodes, while following endpoint security best practices.
- **Incident response and management strategy.** If and when an organization suffers a security event, it needs a preestablished incident response (IR) and management strategy to mitigate risk to the business. Since the fallout from a data breach can include financial losses, operational disruptions, regulatory fines, reputational damage and legal fees, an IR team needs a combination of executive, technical, operational, legal and public relations expertise. This group documents the *who, what, when, why* and *how* of its anticipated IR, creating a plan that will offer clear direction in a future crisis.
- **Network segmentation.** Segmenting the network limits how far cybercriminals can move if they do manage to get inside a network. This will mitigate the damage and scope of an attack.
- **Password policy.** Simplistic or recycled passwords are practically an open invitation to hackers. Creating a company password policy helps protect enterprise security by establishing rules, requirements and expectations around user credentials.
- **Patch management.** Patch management is the flossing of cyber hygiene: Everyone knows they should do it, but not everyone does. And just as a failure to floss may increase the risk of heart disease, failing to patch increases the risk of serious security incidents. In a 2019

Ponemon Institute survey, for instance, 60% of data breach victims confessed they could have kept their attackers out of their systems simply by patching known security flaws. In other words, the stakes are high, so it's critical to understand and follow patch management best practices.

- **Secure remote access.** According to Metrigy's "Workplace Collaboration: 2021-22" report, 84% of organizations plan to permanently let employees work from home, at least part time, after the pandemic. That means secure remote access will continue to be of critical importance in the vast majority of enterprises. A variety of technologies -- including CASBs, firewalls, VPNs, Secure Access Service Edge and zero-trust network access -- can help facilitate secure connectivity for users irrespective of their physical locations.



Top cybersecurity training topics

Here are four crucial topics that should be explored in any security awareness training effort.

Phishing attacks
One of the oldest and still most effective threats, employees must be educated to recognize and handle these security threats appropriately.

Social engineering attacks
Social engineering attacks don't just come in emails, but also from behind a customer service desk, via telephone calls or from the next cubicle. Teach employees to recognize all types.

Password hygiene
A constant battle but a winnable one if you encourage the use of password managers and strong, unique passwords for each site employees visit.

Secure remote work practices
A huge issue for a large population of workers in the wake of COVID-19. Corporate policies on storing and accessing sensitive information must be hammered home.

SOURCE: MIKE CHAPPLE; ICONS: MIAKIEVY/GETTY IMAGES

- **Security awareness training.** Educate employees on the crucial role they play in mitigating cyber-risk by building an effective cybersecurity training plan, suggested Mike Chapple, senior director of IT service delivery at the University of Notre Dame. The most effective security awareness training programs find fresh ways to engage employees in foundational cybersecurity practices. End users can then put their new knowledge to the test with this security awareness quiz.

- **Security log management.** A cybersecurity program is only as good as its ability to recognize inappropriate or suspicious activity in the IT environment. That makes security logging "the heart of any security strategy," according to security expert and author Michael Cobb. But that doesn't mean it's easy. Best practices for security log management include logging and storing the right events, ensuring the accuracy and integrity of logs, analyzing log data to identify problems and using logging tools to manage event volume.
- **Security monitoring.** Regularly or continuously scan the network for threats and vulnerabilities, such as open ports that hackers could use in port scan attacks, using tools such as SIEM or vulnerability scanners. Frequent scanning and monitoring dramatically improves cyber hygiene by flagging both potential active threats and points of weakness where attackers could gain access.

CYBER HYGIENE AND EMAIL SECURITY

Despite the rising popularity of collaboration platforms, such as Microsoft Teams and Zoom, the vast majority of organizations still rely on email as their primary mode of communication. As a result, email remains a popular attack vector for cybercriminals who exploit it to access corporate networks and data. In fact, in the 2021 Data Breach Investigations Report, Verizon researchers found the number of business email compromise (BEC) breaches doubled over the previous year.

In this handbook:

Email security is an array of technologies, techniques and practices to keep cybercriminals from gaining unauthorized access to email accounts and message content. And like all cyber hygiene measures, email security is the joint responsibility of organizations and individuals.

Email spoofing
Jean Quinn
From: ~~Kelly Adams~~
Sent: 4/11/19 9:13 AM
To: Keith Jones
Subject: Data

ILLUSTRATION: AI STUDIO/ADOBE STOCK, INTARARIT/ADOBE STOCK
©2019 TECHTARGET. ALL RIGHTS RESERVED

At the organizational level, establishing an email security policy that is effective and up to date should be a top priority, according to Andrew Froehlich, president of West Gate Networks. Informative, clear and concise policies establish cultural norms and set behavioral expectations around the safe use of email. It's important to outline email's inherent risk and dispel any false sense of security employees might have in using this ubiquitous technology.

On the technical side, IT leaders must understand the importance of leading email security protocols and how they can help keep corporate messages secure. Antimalware, antispam, email security gateways and email filtering can further mitigate the risk of phishing and BEC attacks.

It's important to remember that good cyber hygiene is not a set-it-and-forget-it proposition. Rather, it encompasses a dynamic array of habits, practices and initiatives on the part of organizations and users, with the goal of achieving and maintaining the healthiest possible security posture.