Security Awareness:

7 Security Tips to Use Now

CONTENTS

Low-risk employees

serve as advocates for IT security – they support identifying security threats and reporting them. What can we do to minimize the risk to all employees? Security awareness training.

1 PASSWORDS

Managing passwords is the simplest, most impactful thing you can do when it comes to IT security.

Reset Every Three Months

- Network Logins
- Operating Systems Login (Windows, Linux, MacOS, etc.)
- Email Accounts
- Network Devices (Routers, firewalls and VPNs)
- Wireless Networks (Private and guest access)
- Cloud and data storage services

Essentials: Password Rules

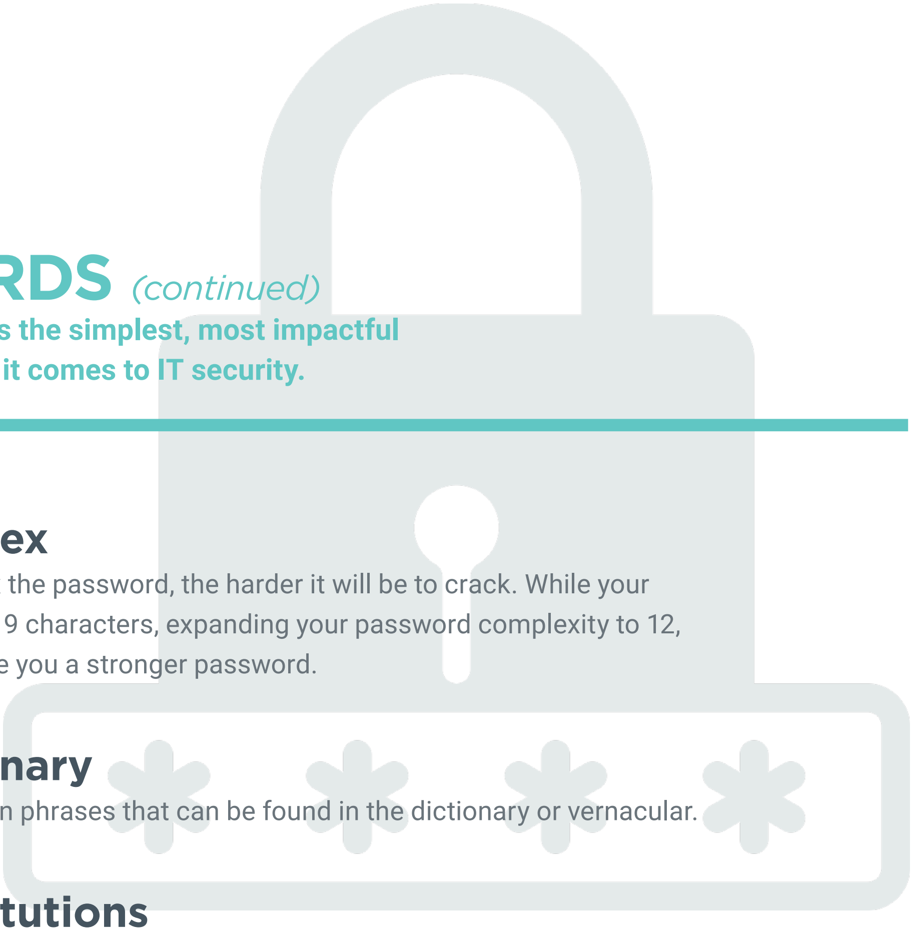
- Characters: upper and lowercase letters
- Numbers
- Special characters (.!@#$%^&*)
- Don’t reuse old passwords

Password to Avoid

- Personally identifiable information
- Public information
- Public information on your social media profiles
- 123456789
- Qwerty
- Password
- 11111
- Abc123
- Iloveyou
- Superman
- Batman
- Sunshine
- Admin
- Welcome
- Princess
- Football
- Baseball
- Names of favorite sports teams
- Usernames

PRO TIPS

- Set your password policy to require changes every 90 days based on the guidelines recommended above.
- Ensure SaaS solutions enforce periodical password resets and support multi-factor authentication (MFA).
- Consider using password managers when allowed to securely store and manage your passwords.



1 PASSWORDS *(continued)*

Managing passwords is the simplest, most impactful thing you can do when it comes to IT security.

Long and Complex

The longer and more complex the password, the harder it will be to crack. While your account may only require 6 to 9 characters, expanding your password complexity to 12, 16 or more characters will give you a stronger password.

Not in the Dictionary

Avoid single words or common phrases that can be found in the dictionary or vernacular.

Character Substitutions

Substituting characters for letters is a good practice, but you want to think outside of the box. Don't substitute zero for the letter O and assume you are safe. A better option would be using the ampersand (&) for O.

Illogical Phrases

While you wouldn't want to use a common phrase like "ThankYouVeryMuch," you could string together completely random words like "ThankCheeseBoatsNetwork."

Acronyms and Abbreviations

Instead of spelling out words, abbreviate them or replace phrases with acronyms that you can remember. Using the example above, "ThankYouVeryMuch" could become "TkYVreM." Of course, you would add more to it so it's longer and has a variety of characters.

PRO TIPS

- Be sure to address legacy systems as part of your password policy.
- Don't make exceptions for executives – they are more frequently targeted by hackers.

2 EMAIL

Email is still the number one entry point for cyber threats. Review email domains, URL links, sender and recipient information as well as the email body content to detect a possible fake email.

Use Spam and Phishing Filters

Most email services offer built-in spam and phishing filters. Make sure these are enabled to automatically detect and filter out potential threats. Regularly check your spam folder to ensure legitimate emails aren't being filtered out.

Be Cautious of Suspicious Emails

Always be wary of emails from unknown senders or those that seem out of the ordinary. Be particularly cautious of emails that ask for personal information, prompt you to click on a link or download an attachment. These could be phishing attempts designed to steal your information or infect your system with malware.

How To Recognize a Phishing Email

Proactive security awareness involves checking the email's domain, address, sender information and the body of the email for anything suspicious. Here are some phishing email red flags to watch for:

- **Urgency:** Any email that prompts you to take action with wording such as "log in immediately," "click here now" or "action required" is likely fraudulent. Most emails do not require this sense of urgency.
- **Wire transfer/receipt of payment:** Before opening an attachment (i.e., invoice) or clicking a link, contact the sender directly to verify email legitimacy.
- **Unusual grammar:** Inspect the email for typos, grammatical errors, unusual tone or wording that clash with company culture.
- **Multiple embedded links:** An email with several embedded links distributed throughout is most likely spam or a phishing attempt. Delete any spam and report any attempted phishing emails.

PRO TIPS

- Implement company-wide email usage policies as part of your Internet use guidelines and cybersecurity policies.
- Use security awareness solutions that routinely train and test users to recognize phishing attempts.

3 NETWORK SEGMENTATION

When it comes to cybersecurity, there is no substitute for network segmentation.

Areas to Segment

- **Users:** Privilege levels should be based on the user's role in device administration.
- **The DMZ:** These subnetworks expose externally facing systems.
- **Guest network:** Keep guest access separate from corporate access.
- **IT workstations:** Give IT their own network segments for testing and management functions.
- **Servers by application:** Create separate network segments for servers with confidential or financial data applications on them.
- **VoIP/communications:** This network will become a common attack plane as communications move away from traditional platforms.
- **Traditional physical security:** Cameras, ID card scanners and other physical devices should run on an independent or firewalled network.
- **Industrial control systems:** In addition to segmentation, remote access by vendors should use VPNs and have MFA.

TERM TO KNOW

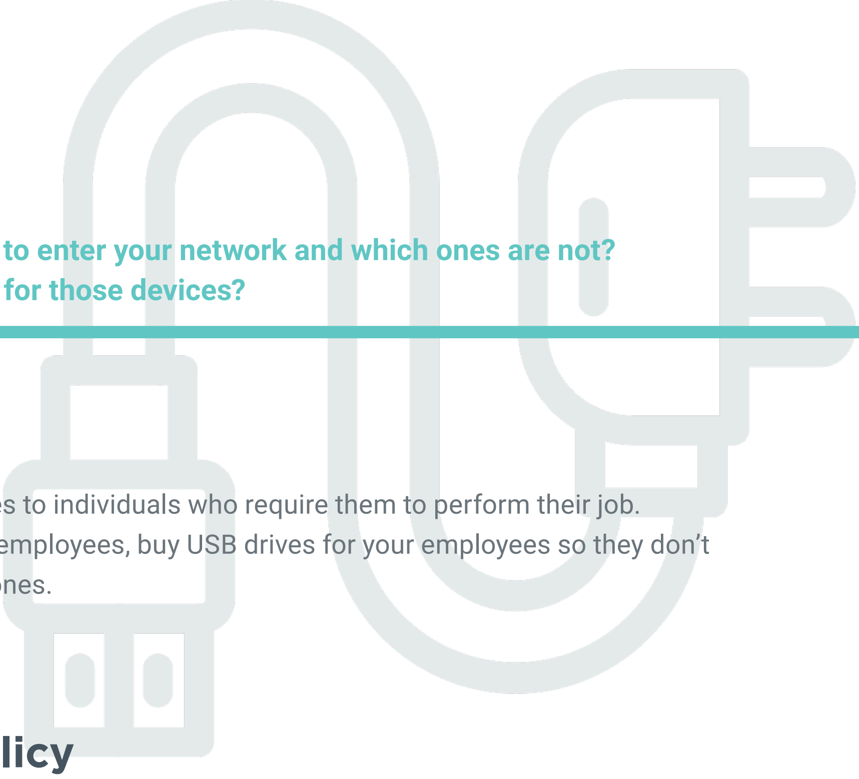
Network Segmentation

Network segmentation is when different parts of a computer network are separated by devices like firewalls, switches and routers. This helps to limit access to those who need it and protect the network from widespread cyberattacks.

PRO TIPS

- Audit your existing network architecture and use the list on this page to figure out your network segmentation priorities.
- Evaluate what resources you'll need to properly segment your network.
- Create a business case to help executives understand why this is important and the time and resources it will require.
- Communicate to end users about what you're doing, why you are doing this, how long it will take and what downtime they may experience.
- Backup EVERYTHING before making any changes.

4 DEVICES



What devices are allowed to enter your network and which ones are not? What policies do you have for those devices?

USB Drives

- Restrict the usage of USB drives to individuals who require them to perform their job.
- If USB drives must be used by employees, buy USB drives for your employees so they don't feel like they need to use free ones.

TERM TO KNOW

Acceptable Use Policy

A corporate acceptable use policy explains what devices can and cannot access the company network and how they can be used while on the network. While an organization's IT staff can control internal devices, such as company-issued laptops and mobile phones, they have less control over external devices like USB drives, personal mobile phones and personal laptops. An acceptable use policy returns control to the IT department and educates employees on how they can best protect the company network.

BYOD (Bring Your Own Device)

- IT should have the ability to quarantine any device regardless of who purchased it.
- Research sample BYOD policies to write and implement your own.

PRO TIPS

- Utilize the operating system's whole disk encryption services when available on all company-issued laptops to help prevent criminals from stealing information on those devices, as well as biometric authentication solutions when available.
- Regularly update the applications and operating system patches to reduce the risk of a cyber-attack from the use of old and vulnerable software.

5 PRIME TARGETS – FINANCE AND EXECS

Finance employees and executives are targeted much more frequently than other teams on your staff.

Protocol Awareness

Finance and executives should understand how the company executes a transfer and the protocol for doing so. Anything outside of that framework should raise suspicion and be reported to IT or the security team. Don't forget to establish policies and procedures for vendors and clients to change banking information. Let them know the process and how you will verify the validity of a request.

Authentication Tokens

Consider requiring an authentication application or a physical authentication token to complete multi-factor authentication.

Executive Triage Training

Executives will have to bear the public relations hit when/if an incident occurs. Is anyone on staff trained on how to deal with this? Do you work with a PR firm, and do you have an incident response plan?.

PRO TIPS

- Create an acceptable transfer policy or refresh your current policy to include these rules.
- Hold a meeting and train on it, then role play a few situations with the staff.
- Audit with finance managers and executive assistants quarterly, looking through transfer requests to see if the protocol was acted on.

6 BACKUP AND RECOVERY

Regularly backup systems and ensure you routinely test the recovery process. In the event of a data breach or ransomware attack, having a backup can save your business.

ESSENTIALS

- **Regular data backup:** Regularly backup all important business data. This includes documents, databases, software configurations and any other critical data.
- **Use automatic backup solutions:** Consider using automatic backup solutions to ensure consistent backups. These solutions can be scheduled to run at convenient times, like after business hours, to minimize disruption.
- **Offsite and onsite backups:** Store backups securely in multiple locations. Onsite backups are convenient for quick recovery, but offsite backups (including cloud-based solutions) protect against physical damage to your business premises.
- **Recovery testing:** Regularly test your backups to ensure data can be recovered. This involves restoring a file from backup and checking its integrity. Backup verification is crucial to ensure your backup system is working correctly.

PRO TIPS

- When backing up systems, utilize encryption capabilities when available and separate passwords for those backups to reduce the risk of data breaches.
- Where possible, look for systems that offer immutable backups to ensure that no one can make changes to the backup after it is made.

7 INCIDENT RESPONSE PLANS

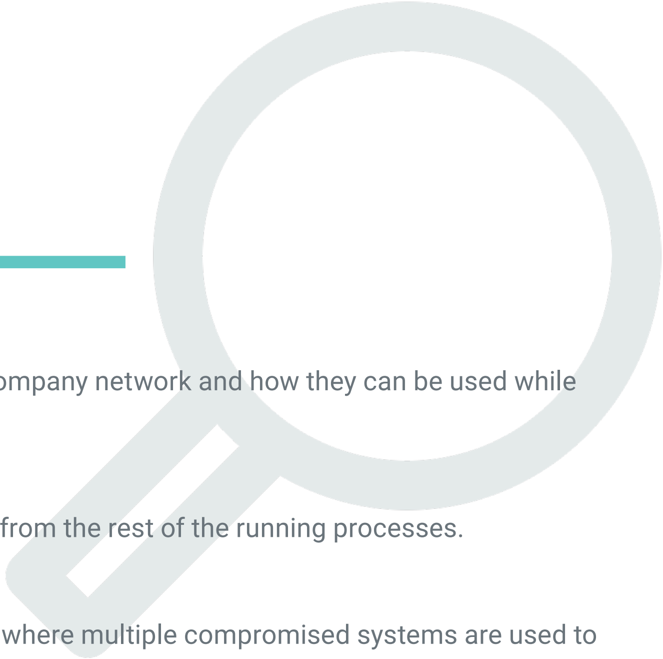
Create an incident response plan that includes the five key areas below.

ESSENTIALS

- **Identify critical systems and data:** Understand where your risks are and what systems are involved internally, in the cloud and with third parties.
- **Form the teams and define the roles:** Identify and assign the individuals or groups that will be involved in a response and clearly define their roles. This can include third-party response groups.
- **Create the action plans for each incident type:** Clearly define the steps and responsible parties for each type of incident. These should include identifying, assessing, containing and recovering.
- **Define a communication/information sharing plan:** Create a clear and effective plan to communicate with both internal and external groups. This should include a chain of command to prevent unauthorized communications, and it may involve law enforcement.
- **Training and testing:** Plans won't be effective if the people involved don't train for and test them. Utilize these exercises to fine-tune and update plans, as situations can change and preparedness is crucial. Don't forget to include training for all employees. In the event they identify an incident, they'll need to know what actions to take and whom to notify.

PRO TIPS

- Ensure your attorney has reviewed any response plans to ensure it complies with all state, federal and international laws and regulations that may apply.
- Hold routine tabletop exercises to run through possible scenarios that may occur and update the plan with any discovered weaknesses.



TERMS TO KNOW

Acceptable Use Policy
Explains what devices can and cannot access the company network and how they can be used while on the network.

Application Isolation
The separation of one program or application stack from the rest of the running processes.

DDoS Attack
Distributed Denial of Service: A type of DDoS attack where multiple compromised systems are used to target a single system.

Domain
A group of computers and devices on a network that are administered as a unit with common rules and procedures; defined by an IP address.

Immutable Backup
An immutable backup is a backup that, once created, cannot be altered or deleted.

Legacy System
Outdated computer systems, programming languages or application software that are used instead of upgrading to available new versions.

Local Area Network (LAN)
A computer network that links devices within a building or group of adjacent buildings.

Multi-Factor Authentication (MFA)
A security process in which the user provides different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access.

Network Segmentation
Network segmentation is when different parts of a computer network are separated by devices like firewalls, switches and routers. This helps to limit access to those who need it and protect the network from widespread cyberattacks

Phishing
The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Ransomware
A type of malicious software designed to block access to a computer system until a sum of money is paid.