

SECURITY AWARENESS

7 Security Hacks to Use Now



CONTENTS

Passwords	3
URLs	5
Email	6
Network Segmentation	7
Devices	8
Prime Targets – Finance and Execs	9
Incident Response Plans	10
Terms to Know	11



Minimal-risk employees are advocates for IT security – they understand and report security threats and breaches. How do we ensure all employees are minimal risk? ***Security awareness training.***

1. PASSWORDS

Managing passwords is the **easiest**, most impactful thing you can do when it comes to IT security. *(And it's free!)*

Reset Every Three Months

- Windows login
- Email/Office 365
- Routers and firewalls
- Other hardware
- Customer relationship management (CRM)
- Marketing automation

< PRO TIPS >

- Set your policy on password resets for every 90 days following the guidelines above.
- Ensure SaaS forces password resets and supports two-factor authentication.
- Be vigilant about the APIs your employees are asking for, and conduct thorough investigations.
- Maintain firmware updates for routers and firewalls.

ESSENTIALS

Password Must-Haves

- Upper and lowercase numerals
- Numbers
- Special Characters i.e. !@#\$%^&*()

Passwords to Avoid

- [personal information of any kind]
- [anything on your social media profiles]
- 123456
- 123456789
- Qwerty
- Password
- 111111
- 12345678
- Abc123
- 1234567
- Password1
- 12345
- Iloveyou
- Superman
- Batman
- Sunshine
- Admin
- welcome
- Princess
- Football
- baseball
- [names of sports teams]

1. PASSWORDS *(Continued)*

Managing passwords is the **easiest**, most impactful thing you can do when it comes to IT security. *(And it's free!)*

Kay@kHouse\$293

!@#\$%^&*()

ThankCheeseBoatsNetwork

TkYVreM

Gr8WhetheR#

< PRO TIPS >

- Anything that houses customer data must comply with General Data Protection Regulation (GDPR) and have strict two-factor authentication.
- Be sure to address legacy systems as part of your password reset.
- Don't make exceptions for executives – they are more frequently targeted by hackers. ***Skip to the Prime Targets – Finance and Executives section for more on this topic.***

ESSENTIALS

Strong Passwords

- **Long:** The longer the password, the harder to crack. While your account may only require 6 to 9 characters, expanding to 12, 16 or more 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.

2. URLs

Train your employees to **pay attention to the address bar** in their browser, and they'll learn how to quickly identify fake websites.

Be on the Lookout

Is your connection secure?

Check the far left of the address bar for a padlock icon to indicate your connection is safe. Chrome and Firefox are safer browsers than Internet Explorer.

Does the URL make sense?

Inspect the link for special characters or numbers and ensure the domain matches that of the company's main site.

Never trust a link in an email, ever.

Call or compose a new email to the person who sent you the link to verify it is legitimate.



< PRO TIP >

Create your own bogus (but harmless) website and send it to your own employees. Track the emails sent to see who opens them, clicks the links or reports them. Implement security awareness training for users who click through but don't report the suspicious email.

3. EMAIL

Bogus emails attempt to trick end users into a sense of comfort, security and legitimacy. Inspect email **domains, names** and **body content** to detect a phishing attack.

HOW TO

Identify Fake Email Addresses

- If the domain is anything different than what you would type to access it from a search bar without any prompt, it's most likely a bogus email.
- The sender can use any names they like. Do not gauge the legitimacy of an email by sender name alone.



< PRO TIP >

Draft emails containing one or all the features* listed above and send them out from both your own legitimate email address and from a dummy account (created for this training). Remember to use a fake email address with your real name and see if that trips anyone up. Hopefully the open rates will be nonexistent on the dummy account.

**For a link-specific exercise, use a trackable link in the body of the email. Check the link activity to see who accessed it.*

HOW TO

Recognize a Phishing Email

Security awareness involves checking the email's domain, address and body of the email for suspicious behavior. Here are some red flags to watch for:


- **Urgency:** Any email that says “log in immediately,” “click here now” or “action required” is bogus. Nothing via email is urgent.
- **Wire transfer/receipt of payment:** Before opening an attachment (i.e., invoice) or clicking a link, call the sender to verify that it is legitimate.
- **Uncharacteristic language:** Inspect the email for typos, unusual tone or language that clashes with company culture.
- **Multiple links:** An email with links sprinkled throughout is most likely spam. Delete it and move on.

4. 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 switching administration.
- **The DMZ:** These subnetworks expose externally facing systems.
- **Guest network:** Keep guest access separate from corporate access.
- **IT workstations:** Give IT their own internet circuit for testing and non-administrative work.
- **Servers by department:** Create a public drive and a private drive for each department.
- **VoIP/communications:** This network will become a more common attack plane as communications move toward more APIs and SaaS platforms.
- **Traditional physical security:** Cameras, ID card scanners and other physical devices should run on an independent network.
- **Industrial control systems:** In addition to segmentation, HVAC (for example) should have two-factor authentication.



Is moving to the cloud a legitimate strategy for network segmentation?

[Click to read more >](#)

TERM TO KNOW

Network Segmentation

Network segmentation is when different parts of a computer network are separated by devices like bridges, 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.
- Back up EVERYTHING before making any changes.

5. DEVICES

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

USB Drives

- These should always be pretested on a segmented machine separate from the rest of the network.
- Buy USB drives for your employees so they don't feel like they need to use free ones.

Always throw out a free USB drive.

< PRO TIP >

Leave free USB drives scattered around the office with a macro-enabled file on them that will alert you when opened. All of the offenders need to be trained on this point specifically.

Think it won't work? The FBI conducted a similar exercise, leaving 10 USB drives in the parking lot. Half of them were plugged in on FBI machines.



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.



6. PRIME TARGETS Finance and Execs

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

Protocol Awareness

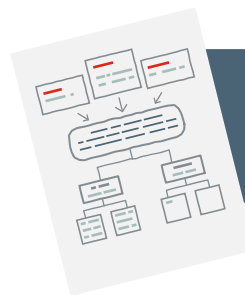
Finance and executives should know how your company typically executes a transfer and the protocol for doing so. Anything outside of that framework should raise a red flag and be reported to IT.

Authentication Tokens

Consider requiring a hard token that plugs into a laptop or other device's USB port to complete two-factor authentications. Sometimes there's no substitute for a physical barrier.

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?



Don't have an incident response plan?

[Click to learn more >](#)

< PRO TIP >

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.



7. INCIDENT RESPONSE PLANS

Create an incident response plan, then take your employees and the executive suite through a **breach incident exercise**.

➤ First Responders

Power off: Segment, power off and disconnect the ethernet cord from the machine in question.

Don't delete it: Keep the suspected malicious file for inspection by a forensic investigator.

Communicate up: Detail who first responders should notify and their next steps in the event of a breach.

➤ Front-Line Managers

Managing teams: How (if at all) should teams continue working?

Managing customers: Create a template email to notify clients in case of an incident affecting them.

➤ Marketing

Create an emergency kit should a breach occur:

- Social media posts to inform and reassure
- Email draft informing customers and supply chain of the incident
- Email drafts for employees to personally send to customers
- Shareholder email drafts (if applicable)
- Schedule detailing the frequency of updates sent to customers and supply chain moving forward

V Threat actors are notoriously lazy.

Hackers are looking for the least-trained lowest common denominator when it comes to end users. **Security awareness training is your front line of defense.**

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

General Data Protection Regulation (GDPR)

A legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU)

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

Network segmentation

When different parts of a computer network are separated by devices like bridges, 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

Two-factor authentication

A security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access