

Cybersecurity Awareness Training Facilitator Guide



TABLE OF CONTENTS

Overview2

Preparation & Planning4

Facilitator’s Guide5

 Welcome & Introductions5

 Introduction to Cybersecurity Awareness7

 Social Engineering Awareness10

 Social Engineering Prevention Strategies20

 Learning Checkpoint #123

 Social Media Compromise & Safety24

 Learning Checkpoint #229

 Stay Cyber-Safe When Working Remotely.....33

References.....36

Overview

About the Document

How to use this document

This document is to be used as a guide for leading a training on cyber security awareness. The order of topics is strategic and outlines the talking points for each slide in the presentation. A section is available at the end which references additional resources if the trainer wishes to read more about the specific topics covered.

Links to outside sources, including the video clips included within the presentation, are noted with each slide.

Time estimations are included for each section. Where reasonable, sample wording is provided to introduce a topic but is there only as a guide for a new facilitator. Each topic includes key points.

The guide is organized in the same order as the slide presentation. It provides snapshots of each slide throughout the document.

About the Training

Training Schedule Overview

Time	Section
30 minutes	Welcome and icebreaker activity (if in-person)
	Introduction to topic
1.25 hours	Social engineering scams and attacks
15 minutes	Break
1.5 hours	Social engineering prevention strategies
1 hour	Lunch
1 hour	Social media compromise and safety
15 minutes	Break
30 minutes	Stay cyber-safe when working remotely
15 minutes	Closing remarks

Objectives for this Training

The participants will:

- Be able to identify common social engineering tactics and how to avoid them.
- Know what it means to be safe when engaging in social media.
- Understand how to stay protected while working (and playing) online.

Participants

This is a bi-yearly training intended to be delivered to all employees once per year and for new hires as part of the new employee orientation conducted during their start week. Employees are required to complete this training regardless of their position.

Delivery

This training is designed to be flexible enough to be delivered in person or online using Microsoft Teams. PowerPoint slides are provided to direct the training session. In either case, a wireless or hard-wire connection is required to be able to view the training videos and online learning activities embedded into the PowerPoint presentation.

In addition, there are a few sections where options are presented for different activities. The trainer may use one, some, or all of the options (if desired).

Pre-Training Preparation

In preparation for training on this topic, it is recommended that the trainer review the information on the following websites:

- National Cybersecurity Alliance: <https://staysafeonline.org/cybersecure-business/>
- Stop. Think. Connect. <https://stopthinkconnect.org/>
- Anti-phishing Work Group: <https://apwg.org/>
- Cybersecurity & Infrastructure Security Agency: <https://www.cisa.gov/publication/cisa-cyber-essentials>
- Center for Development of Security Excellence: <https://www.cdse.edu/Training/Cybersecurity/>

Preparation & Planning

Preparation Checklist

- ☐ Complete pre-training preparation.
- ☐ Prepare participant workbooks.
- ☐ Prepare activity handouts.
- ☐ Email participant workbook and activity handout if session will be conducted online.
- ☐ For in-person training only: Procure Lego bricks of various sizes (10 per person attending).
- ☐ Review presentation slide deck.

Agenda

Time	Section
30 minutes	Welcome and icebreaker activity (if in-person)
30 minutes	Introduction to cybersecurity awareness
	What is the difference between the internet and the dark web?
	Surprising social engineering statistics
	Amazing social media statistics
1.75 hours	Social engineering scams and attacks
	Phishing
	Vishing
	Smishing
	Business Email Compromise
	Quid pro quo attacks
	Scareware
	Watering hole attack
	What to do if you become a victim
15 minutes	Break
1 hour	Social engineering prevention strategies
30 minutes	Learning checkpoint
1 hour	Lunch
1 hour	Social media compromise and safety
	Facebook
	LinkedIn
	Twitter
30 minutes	Learning checkpoint
15 minutes	Break
30 minutes	Stay cyber-safe when working remotely
15 minutes	Closing remarks

Facilitator Guide

Welcome & Introductions (30 minutes)

Description The welcome and introduction

Sections

- Welcome statement from trainer (5 minutes)
- Ice breaker activity (if in-person session) (25 minutes)

Materials

- ☐ Participant workbooks
- ☐ Facilitator presentation & notes
- ☐ Legos (for in-person session only)

Welcome (5 minutes)

OVERVIEW Introduce the trainer to the group.

EXAMPLE SCRIPT

Please note: The example script is just a guide. This is meant to provide the newer presenter an idea of what could be said. This script may be adapted to the presenter's own style and voice.

Example:

"Good morning and welcome! My name is _____ and I'm so excited to be leading this training today. I have been with the company for _____ years. Some of my credentials include...."

"This training is designed to provide you with the knowledge and tools you need to be security-aware while you're on the internet and/or working remotely."

"You can expect a lot of information, interesting videos, practice, and self-paced learning activities."

"After today, you'll have the opportunity to take what you learned and apply it right away whether it's here at work, working from home, or in your day-to-day personal activities."

Discussion Starter:

"Who can tell me one thing they're looking forward to learning about today?"

Icebreaker - Introductions (25 minutes)

OVERVIEW	Introduce participants to each other.
OBJECTIVES	Participants have a positive attitude toward topic.
ACTIVITY	Each participant gets a set of 10 LEGO bricks (identical sets to everyone – a few items, around 5-10 bricks per person will suffice). Everyone builds something that relates to the topic of cybersecurity. Afterwards, everyone gets 30 seconds to explain what their building means (e.g 'My Home', 'Interesting Experiment', 'The coolest computer ever') and how it relates to the topic of cybersecurity.

EXAMPLE SCRIPT

Please note: The example script is just a guide. This is meant to provide the newer presenter an idea of what could be said. This script may be adapted to the presenter's own style and voice.

For example:

1. Distribute LEGO kits.
2. Spend 5-10 minutes building something that relates to the topic of cybersecurity.
3. After 5-10 minutes, we will come back together and each person will have 30 seconds to introduce themselves (name, title, department) and explain the object they built with their LEGOs.

For example:

"To kick off the day, we're going to be playing with LEGOs! For the first part of this activity you are going to take 5 to 10 of your LEGOs and build something that relates to the topic of cybersecurity.

You will have 5 to 10 minutes to do this, depending on when people finish. Afterwards, each of you will get 30 seconds to introduce yourself. You'll tell us your name, title, and department. Then you will explain what your LEGO structure is and how it relates to cybersecurity."

Introduction to cybersecurity awareness (30 minutes)

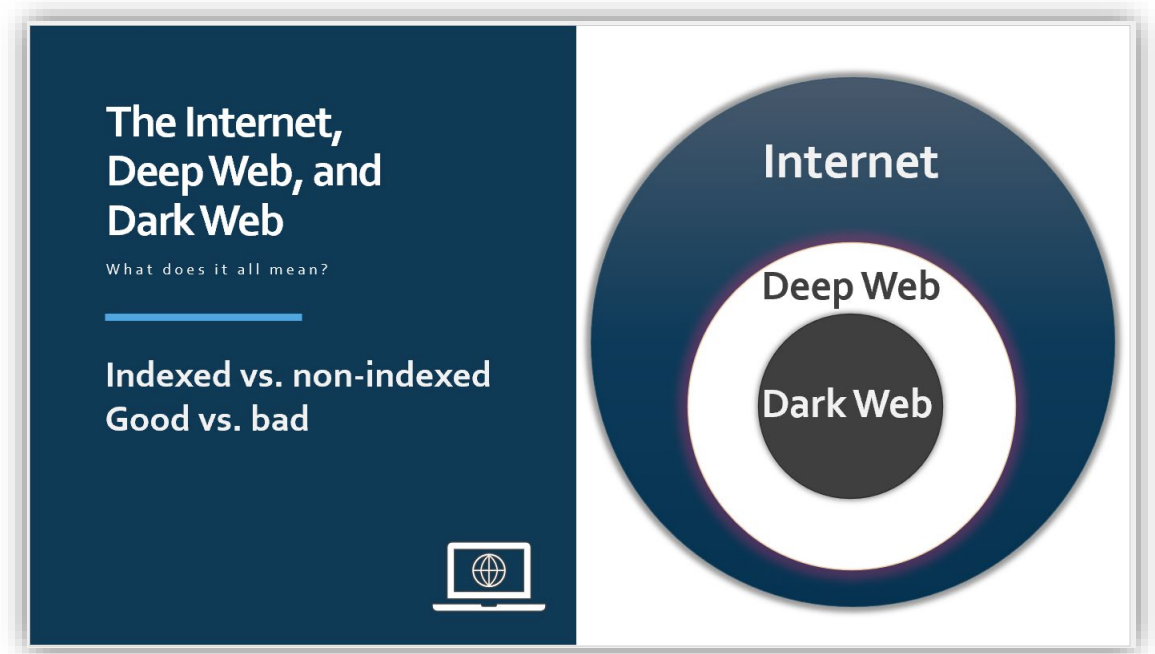
Description Introduce the topic of cybersecurity awareness.

Sections Difference between the internet and the dark web (10 minutes)
Surprising social engineering statistics (10 minutes)
Alarming social media statistics (10 minutes)

Materials ☐ Facilitator presentation & notes

Difference between the internet and the dark web (10 minutes)

OVERVIEW Discuss the difference between the internet and the dark web.



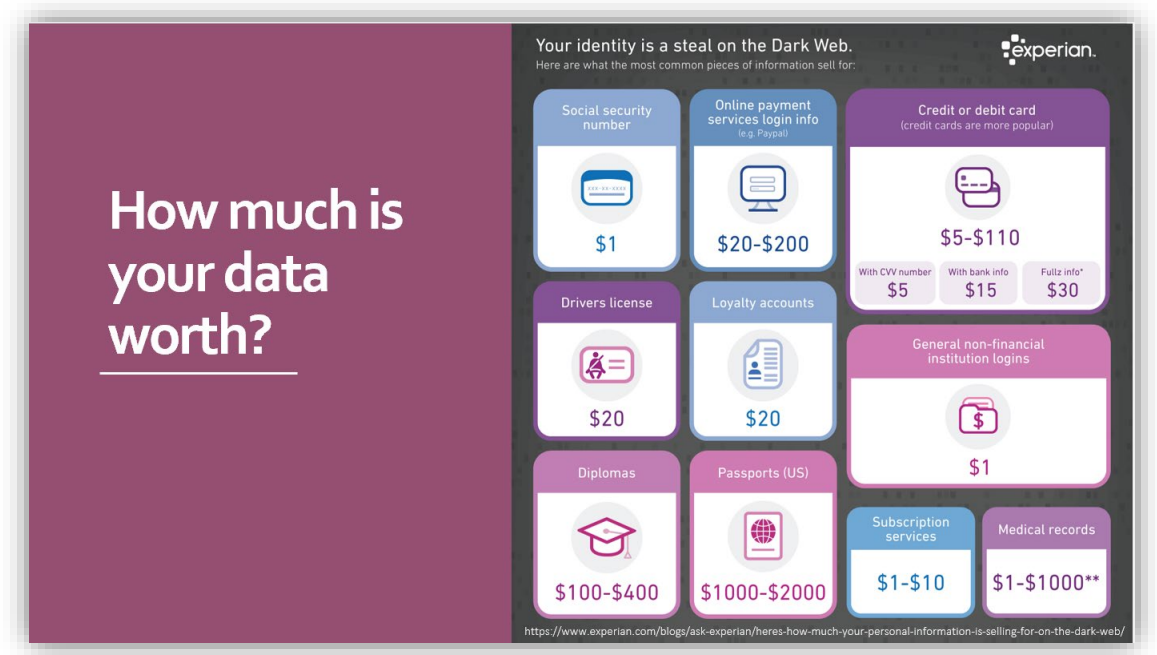
KEY TAKEAWAYS

- The Internet is what we know as “surfing the web” or browsing with Google, Duck Duck Go, Bing, Safari, and other browsers.
- Browsers have their own indexes of the web.
- The Internet is too large to be fully indexed and the sites that do not get indexed are categorized as the Deep Web. The Deep Web is NOT malicious.
- The Dark Web is a sub internet of the Deep Web. It is also not indexed. It is extremely private and access can only be done through special types of browsers. The Dark Web can be VERY malicious and is where illegal activities are conducted.

Surprising social engineering statistics (10 minutes)

OVERVIEW

Discuss how much data is worth on the dark web.



KEY TAKEAWAYS

- There are three ways personal information is sold on the Dark Web: a single record, in bulk, or bundled.
- Four factors that influence the cost of personal information: the type of information, supply and demand, values of the harvested financial accounts, and whether or not the data can be reused.

Amazing social media statistics (10 minutes)

OVERVIEW

Understand the magnitude of social media.

Amazing Social Media Statistics



The smartphone is the device of choice for most US mobile social network users; more than 150 million in United States alone.

An estimated 30 thousand websites a day are hacked.

Approximately 313 million users monthly on Twitter.

Approximately 433 million users on LinkedIn.

Approximately 500 million monthly users on Instagram.

Approximately 176 registered users on Pinterest.

Approximately 256 days to spot a social medial breach.

Approximately 88 days to contain a breach.

Source (2017): <https://www.cdse.edu/Training/Security-Training-Videos/Cybersecurity/Social-Media/>

KEY TAKEAWAYS

- With the millions of social media accounts is growing at an exponential rate but so are opportunities for fraud and data breaches.

Social Engineering Awareness (1 hour, 45 minutes)

Description Identify social engineering tactics

Sections Phishing (20 minutes)
Vishing (10 minutes)
Smishing (10 minutes)
Business email compromise (20 minutes)
Quid pro quo attack (10 minutes)
Scareware (10 minutes)
Watering hole attack (10 minutes)
What to do if you become a victim (15 minutes)

Materials

- ☐ Facilitator presentation & notes
- ☐ Update pie chart graphic with the latest information from <https://blog.knowbe4.com/topic/top-clicked-phishing-email-subjects>. New statistics are published each quarter. Use Windows snipping tool to grab the pie chart information only.

Phishing (20 minutes)

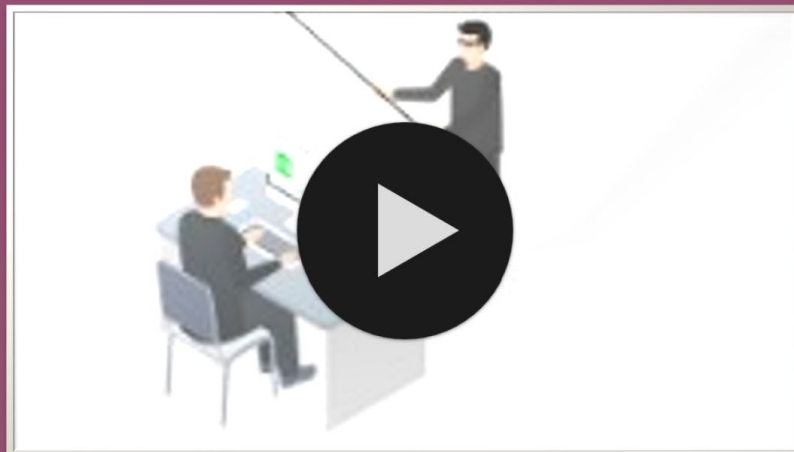
OVERVIEW

Understand what phishing scams are and why they work. Scammers use email to get your sensitive information. Email messages look identical to ones from trusted sources like organizations and people you know.

What is phishing?

<https://youtu.be/Y7zNIEMDml4>

VIDEO – 2 minutes, 56 seconds



Phishing

KEY TAKEAWAYS

- Phishing is a way of trying to gather personal information using deceptive emails and websites.
- Scammer poses as a trusted entity (e.g. person, business, bank, doctor) and tricks victim into providing personal information (e.g., credit card information, account numbers, usernames, passwords).
- Uses fake login pages and email requests. They look VERY real.
- Scammers continue to find new tactics to trick their victims.
- Sometimes offer free items and then tell the victim they need to provide some personal information to be able to receive it.



KEY TAKEAWAYS

- Scammers impersonate popular brands. Google, Amazon, and WhatsApp are the top three brands used in phishing scams.



Note: Update this slide with this quarter's information. Instructions available in preparation details for this section.

KEY TAKEAWAYS

- Scammers impersonate popular brands. Google, Amazon, and WhatsApp are the top three brands used in phishing scams.
- Scammers manipulate their victims through different types of emails. The most popular is business-related email at 25% and the least popular is using current events (2%).

Vishing (10 minutes)

OVERVIEW

Understand what vishing attacks are and why they work. Vishing is phishing but with using voice messages.

Security Awareness Episode 6: Vishing

<https://youtu.be/Hc01oZPvByg>

VIDEO – 2 minutes, 25 seconds



What is Vishing?

KEY TAKEAWAYS

- Vishing is phishing but via voice calls and messages instead.
- Scammers can purchase spoofed phone numbers and blast out messages containing malicious links.
- Do not share personal or company information with someone you are unfamiliar with or are from untrusted sources.
- Report suspicious calls or messages to IT security.

Smishing (10 minutes)

OVERVIEW

Understand what smishing attacks are and why they work. Smishing is similar to phishing except it is done using SMS text messages. Scammers purchase spoofed phone numbers and blast out messages containing malicious links.

What is smishing?

<https://youtu.be/ZOZGQeG8avQ>

VIDEO – 3 minutes, 36 seconds



KEY TAKEAWAYS

- Smishing is similar to phishing except it is done using SMS text messages.
- Scammers purchase spoofed phone numbers and blast out messages containing malicious links.
- Malicious links install malware, share personal information or give away money.
- Smishing scams are more successful than phishing scams – 98% of text messages are read with a 45% response rate vs. email where 20% are read with a 6% response rate.
- Text messaging is easier for the scammer because of the general lack of security on cell phones.
- Banking smishing is the most lucrative tactic.
- Scammers exploit the victim's greed or desperation.
- Pretending to be collecting money for a cause is a popular tactic.

Business Email Compromise (20 minutes)

OVERVIEW

Understand what a business email compromise scam is and why this tactic works. There are two types: impersonation and account compromise.

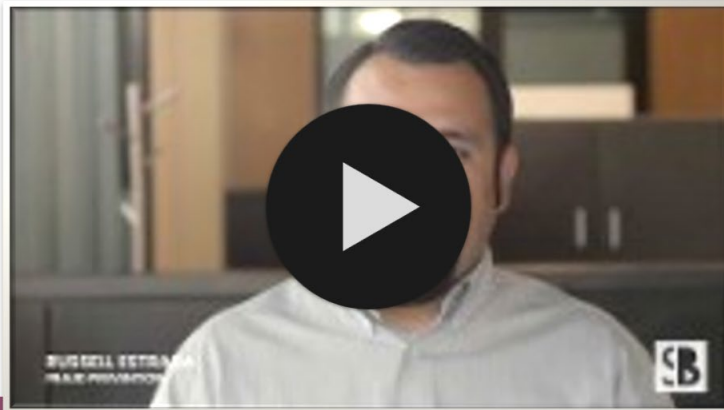
In an impersonation type of scam, the scammer uses a spoof email to pose as an employee or a trusted vendor or customer. The scammer will ask their target to send them payments, change payroll and direct deposit information, or to share other sensitive information.

In an account compromise, a hacker gains access to a legitimate employee's email address and then sends and replies to emails as the employee (e.g., to other employees, customers, and vendors) that include malicious code.

Business Email Compromise Scams Simplified

<https://youtu.be/h3ipCcndIq0>

VIDEO – 3 minutes, 34 seconds



Business Email Compromise

KEY TAKEAWAYS

- A form of theft done via email attempting to get businesses to perform fraudulent wire transfers, ACH transfers, or check payments.
- There are two types of (BEC): Impersonation and account compromise.
 - Impersonation type: spoof emails to pose as employees or trusted vendors and clients. Scammer asks victim to send fraudulent payments, change payroll, direct deposit information, or share sensitive information.
 - Account compromise: Hackers gain access to a legitimate employee email address. Scammers pose as the employee and

can reply to and send emails company-wide (to clients, vendors, etc.), containing malicious code.

- Phishing and malware attacks are sent to the victim through either a hyperlink or an infected attachment. If clicked or opened, the thief gains control of the victim's email account.
- The average bank robber may score \$3,800 in a single robbery but the average takeaway from a BEC scam is more than \$130K.
- In 2018 FBI reported \$12.5 billion loss due to BEC scams and 78K reported incidents.
- Report this type of incident immediately! The chance of recovering the stolen money is unlikely after 72 hours.
- Prevention tactic is security awareness training, implementing 2-factor authentication, changing passwords regularly.
- Never assume a financially-related request is legitimate.

Quid Pro Quo Scam (10 minutes)

OVERVIEW

Understand what a quid pro quo scam is and why this tactic works.

Quid Pro Quo Scams

- Scammers pretend to be from an IT department or other technical service provider.
- Offers incentives (e.g., speed up your internet or fix a computer problem).
- Asks you to create a free account or provide/verify your login credentials.
- Scammer takes this information and uses it against you, sells it on the dark web, or installs malware for an even larger hack.



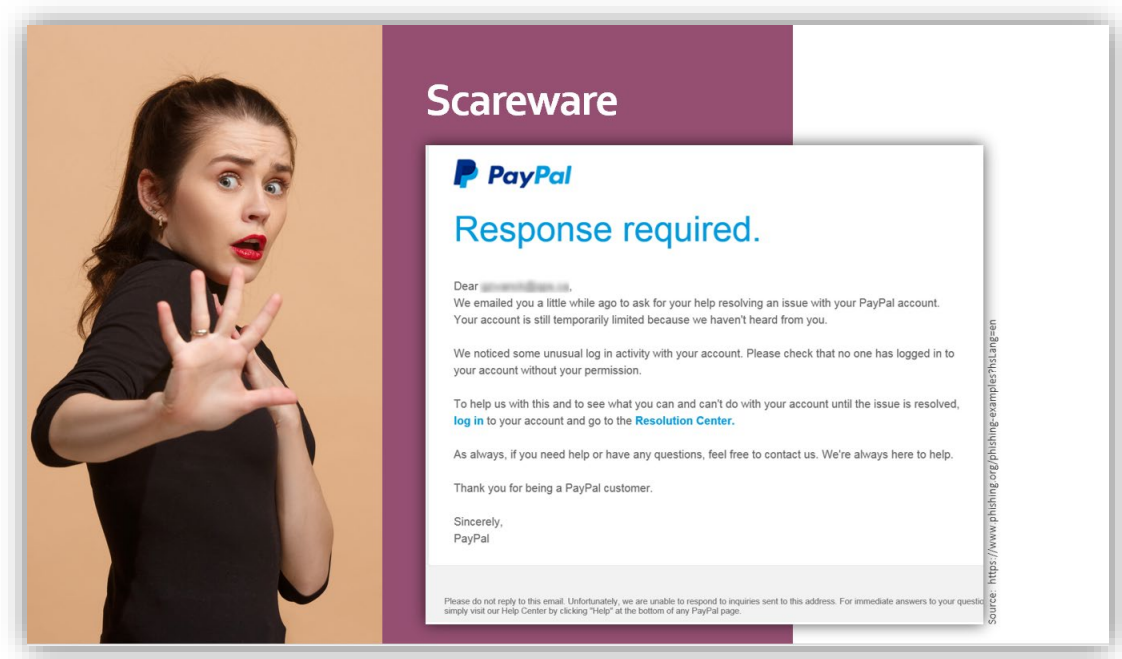
KEY TAKEAWAYS

- “Give and take” exchange type of scam.
- Preys on the fact that humans obey the law of psychological reciprocity.
- Most popular scam scenario is where the scammer pretends to be from an IT department or technical service provider and offer incentives (e.g. speed up your internet or fix computer problem you’re having).
- They will ask you to create a free account or to provide/verify your login credentials and then take the information to use against you, sell on the dark web, or install malware for an even larger attack.
- Precursor to a phishing or ransomware attack.

Scareware (10 minutes)

OVERVIEW

Understand what scareware is and why this tactic works.



KEY TAKEAWAYS

- Also known as fraudware, deception software, or rogue scanner software.
- Gets victim to believe there is some type of imminent danger or threat if they don't comply with the scammers request.
- Example: victim gets a pop-up that they have a virus. Click the button to start a virus scan. The victim gets a virus instead.

Watering Hole Attack (10 minutes)

OVERVIEW

Understand what a water hole attack is and why this tactic works. Hackers infect a site that you regularly visit but when you visit it, your system becomes automatically infected. It can also look like a spoofed site where you enter your credentials (e.g. password and username) that go directly to the hacker.

How a watering hole attack works

https://youtu.be/nNzUg_gW1tI

VIDEO – 3 minutes, 14 seconds



KEY TAKEAWAYS

- People fall victim to a spoofed website, inadvertently giving the attacker their credentials, passwords, bank account numbers, usernames.
- Hackers find a vulnerability in the coding of a website and exploits it to install malware.
- A victim visits the site, gets infected with the malware which gives the hacker control over the victim's computer to do whatever they want.

What to do if you become a victim (15 mins)

OVERVIEW

Sometimes social engineering scams and attacks look so real that you can be fooled no matter how hard you try. What should you do if you become a victim?

Did you click on that link at...

home?



-  Change your passwords for as many accounts as you have.
-  File a report with the Federal Trade Commission (FTC) at <https://reportfraud.ftc.gov/#/>.



Report it immediately to the IT Security hotline or click on the "Phish Report" button on your email task bar.

work?



KEY TAKEAWAYS

- If this occurred using a work email account, report it immediately to the IT Security hotline or click on the "Phish Report" button on your email task bar.
- If this occurred using a personal email account, change your passwords for as many accounts as you have AND file a report with the Federal Trade Commission (FTC) at <https://reportfraud.ftc.gov/#/>.

BREAK
(15 Minutes)

Social Engineering Prevention Strategies (1 hour)

Description Strategies for preventing social engineering scams and attacks.

Sections Social Engineering Prevention Strategies (1 hour, 15 minutes)

Materials ☐ Facilitator presentation & notes

Prevention Strategies (1 hour)

OVERVIEW Stop the social engineering scams and attacks before they start.



The Do's and Do Not's of Cybersecurity Awareness

- ✓ Carefully check email names, addresses, and copy for spelling and grammar mistakes.
- ✓ Stay informed about the latest phishing techniques being used.
- ✓ Always verify the sender of suspicious emails.
- ✓ Report ransomware to the FBI.
- ✓ Report suspicious emails to your IT department.
- ✓ Think before you click.
- ✓ Install an anti-phishing toolbar.
- ✓ Verify a website's security by checking for a padlock icon.
- ✓ Regularly check your financial accounts.
- ✓ Keep your browser and computer patches up to date.
- ✓ Use an antivirus software.
- ✓ Reduce your social media footprint.
- ✓ Use a Virtual Private Network (VPN) connection on your laptop and/or phone.
- ✓ Implement multifactor authentication whenever possible.
- ✓ Register with an identity theft monitoring service.

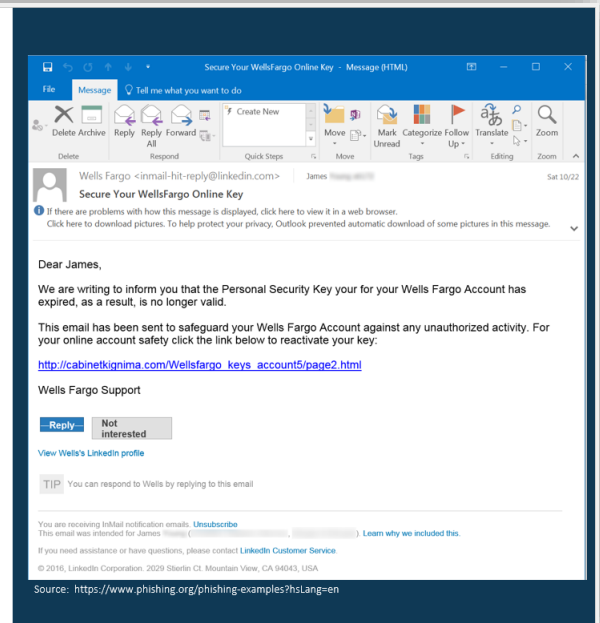


- ✗ Don't open emails from people you don't know.
- ✗ Don't ever respond to ransomware.
- ✗ Don't delete suspicious emails.
- ✗ Don't give out your personal information.

This image by Unknown Author is licensed under CC BY-SA 4.0

Examples of suspicious email subject lines

- Notice: Your online account was accessed
- IRS Tax Transcript
- Celebrate Mom this Sunday with an exquisite bouquet for only \$19.95
- Service cancellation [date]
- SHIPPING DOCUMENT / TRACKING CONFIRMATION
- Confirmation for your delivery
- FBI letter of notification [code 210]
- Incoming fax
- Notice of payment
- Treat as urgent and get back to me
- Your installation
- Your phone number
- Secure your online key



Security Awareness Episode 1: Passwords

<https://youtu.be/0Wd3JoUHXno>

VIDEO – 3 minutes, 9 seconds



Mind your password!

Trick to making a strong (but memorable) password

Use a favorite quote:

You miss 100% of the shots you never take. – Wayne Gretzky

Password becomes: Ym100%otsyntWG



Use a simple sentence:

The first house I ever lived in was on 27th Street in Milwaukee, Wisconsin.

Password becomes: Tfhleliwo27SiMW

KEY TAKEAWAYS

- Password strength is related to length and complexity.
- Passwords should be at least 8 to 12 characters.
- Use upper and lower case letters, numbers and symbols to make the password complex.
- Don't use any words that can be found in the dictionary.
- Don't reuse a password that you had in the past.
- Don't store your passwords in spreadsheets or in the cloud unless you are encrypting the file or putting a password on it.

Learning Checkpoint #1 (30 minutes)

Description

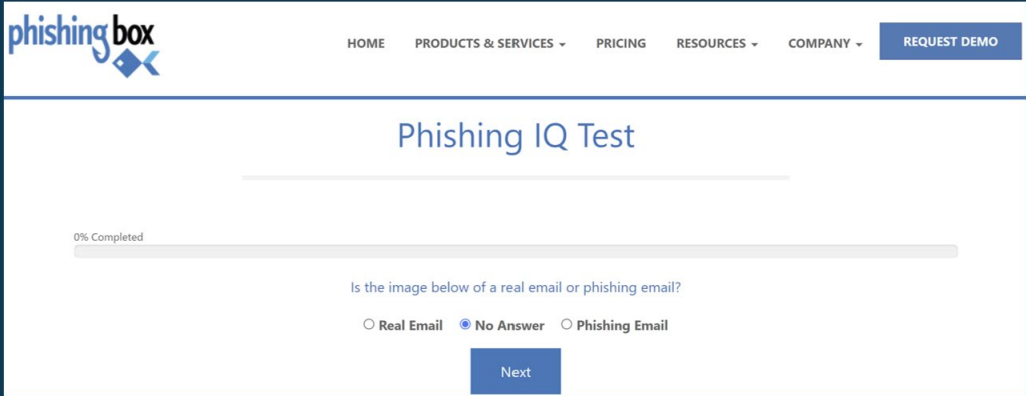
Fake or Real email quiz

Materials

- ☐ Facilitator presentation & notes
- ☐ 3 to 5 giveaway prizes depending on number of participants

Phishing IQ Test

<https://www.phishingbox.com/phishing-iq-test>



The screenshot shows the Phishing IQ Test website. At the top is the Phishing Box logo and a navigation menu with links: HOME, PRODUCTS & SERVICES, PRICING, RESOURCES, and COMPANY. A 'REQUEST DEMO' button is on the right. The main heading is 'Phishing IQ Test'. Below it is a progress bar showing '0% Completed'. The question is 'Is the image below of a real email or phishing email?'. There are three radio button options: 'Real Email', 'No Answer' (which is selected), and 'Phishing Email'. A 'Next' button is at the bottom right of the form.

Open a browser and go to: <https://www.phishingbox.com/phishing-iq-test>

Learning Checkpoint

FACILITATOR NOTES

Participants will take the quiz online. Prizes can be given out for a number of things. Some suggested prize winners: highest score, quickest finisher, department with the most people attending, etc.

EXAMPLE SCRIPT

Please note: The example script is just a guide. This is meant to provide the newer presenter an idea of what could be said. This script may be adapted to the presenter's own style and voice.

For example:

"If everyone would go to the website noted on the slide for our Phishing IQ Test. There's going to be some prizes involved here. So, do your best! Everyone has 15 minutes to complete the test. At the end, please note your score."

We'll circle back after the 15 minutes are up and find out who our winners are."

[AFTER 15 MINUTES...]

“How did everyone do? Everyone stand up. If you had 5 or less right, please sit down. If you had 6 right, please sit down. If you had 7 right, please sit down. If you had 8 right, please sit down. If you had 9 right, please sit down. If you had all of them right, you are the winner!”

[GIVE A PRIZE TO THE WINNER AND THE RUNNER-UP]

[REVIEW THE CORRECT ANSWERS WITH THE GROUP]

LUNCH BREAK (1 hour)

Social Media Compromise and Safety (1 hour)

Description Learn how social media accounts can be hacked. Keep them out!

Sections Facebook (20 minutes)
LinkedIn (20 minutes)
Twitter (20 minutes)

Materials ☐ Facilitator presentation & notes

Facebook (20 minutes)

OVERVIEW Find out how hackers can hack your Facebook account. You can be proactive to prevent from becoming a victim.

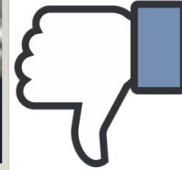
Ten Things You Should Never Share on Facebook

https://www.youtube.com/watch?v=v_MejDubxtQ

VIDEO – 9 minutes, 11 seconds



10 Things You Should Never Share on Facebook



Facebook Safety

Facebook Thumb – Source: https://www.pisimg.com/png/m/5-58587_facebook-thumb-up-is-an-png-thumb-up-facebook.png
Facebook Video – Source: https://www.youtube.com/watch?v=w_MejDubxtQ

KEY TAKEAWAYS

- Remove your phone number if you have it posted on your Facebook page.
- Remove people you no longer stay in contact with.
- Everything (including your preferences) that Facebook knows about you is used for advertising.
- Whatever you Google can end up as Facebook suggestions.
- Go to www.facebook.com/ads/preferences/edit to turn off those preferences off.
- Disable Facebook's facial recognition feature or edit the "who sees tag suggestions" preferences. You may be tagged in photos you don't want to be associated with and not know it.
- Resist the urge to post location check-ins. Your Facebook friends and strangers will know where you are.
- Disable your relationship status.
- Having your birthday posted for everyone to see is information that can be used to access your bank and other personal accounts. Keep your birthday private.
- Do not post any updates while you are on vacation. Anyone who can see your Facebook profile will know you are gone. It increases the likelihood of your house getting broken into. Insurance companies have been known to refuse burglary claims once they found out the homeowner was broadcasting that he or she was out of town.

Center for Development of Security Excellence
CDSE

Facebook Smart Card

Security in an Insecure World

Facebook offers privacy settings for added security

Privacy Settings and Tools

Who can see my stuff?	Who can see my future posts?	Who can contact me?	Who can look me up?
Review all your posts and things you're tagged in	Review all your posts and things you're tagged in	Who can send you friend requests?	Who can look you up using the email address you provided?
Limit the audience for posts you've shared with friends of friends or Public?	Limit the audience for posts you've shared with friends of friends or Public?	Whose messages do I want filtered into my inbox?	Who can look you up using the phone number you provided?
Friends	Friends	Friends	Friends
Use Activity Log	Use Activity Log	Use Activity Log	Use Activity Log
Limit Past Posts	Limit Past Posts	Limit Past Posts	Limit Past Posts
Do you want other search engines to link to your timeline?	Do you want other search engines to link to your timeline?	Do you want other search engines to link to your timeline?	Do you want other search engines to link to your timeline?
No	No	No	No

Always select "Friends" where possible

Privacy Checkup

1. Your Posts
2. Your Apps
3. Your Profile

Always select "Friends" where possible

Source: <https://www.cdse.edu/Portals/124/Documents/jobbaid/cyber/cyb-facebook-smartcard.pdf?ver=9evqdcckfQgOngmwL7OHMOA%3d%3d>

Extracted from:

<https://www.cdse.edu/Portals/124/Documents/jobbaid/cyber/cyb-facebook-smartcard.pdf?ver=9evqdcckfQgOngmwL7OHMOA%3d%3d>

Center for Development of Security Excellence
CDSE

Facebook Smart Card

Security in an Insecure World

Source: <https://www.cdse.edu/Portals/124/Documents/jobbaid/cyber/cyb-facebook-smartcard.pdf?ver=9evqdcckfQgOngmwL7OHMOA%3d%3d>

To deactivate your Facebook account:

Account Settings → Security → Deactivate your account.

To reactivate your Facebook account:

Log in to Facebook with your email address and password.

To delete your Facebook account:

Help → type "Delete" into the search box → select "How do I permanently delete my account?" → scroll down to "submit your request here" → verify that you want to delete your account → "Submit".

Security Settings

Enable login alerts, so you know when your account is accessed

Require approval to log in from new browsers

Check often and delete any unsecured, shared browsers

Check often and remove any unknown active sessions

Timeline and Tagging Settings

Who can post on your timeline?

Who can see things on my timeline?

Always select "Friends" where possible

Extracted from:

<https://www.cdse.edu/Portals/124/Documents/jobbaid/cyber/cyb-facebook-smartcard.pdf?ver=9evqdcckfQgOngmwL7OHMOA%3d%3d>

LinkedIn (20 minutes)

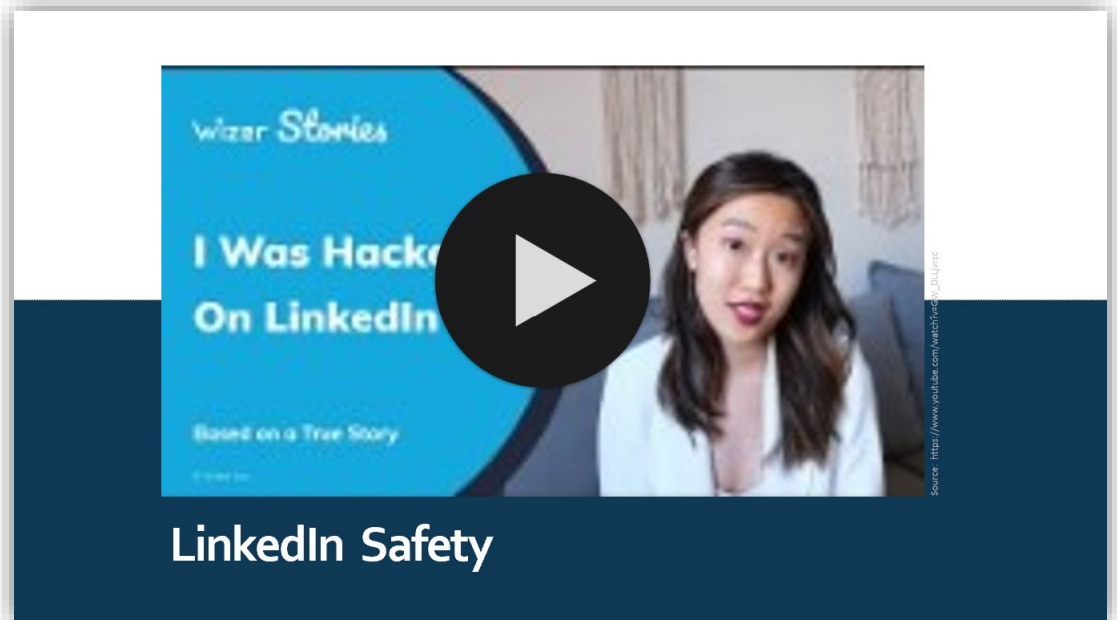
OVERVIEW

Find out how hackers can hack your LinkedIn account. You can be proactive to prevent from becoming a victim.

How I was Hacked on LinkedIn: A True Story

https://www.youtube.com/watch?v=GW_DLLjvrsc

VIDEO – 1 minute, 53 seconds



KEY TAKEAWAYS

- Make sure you turn on two-factor authentication.
- Go through the recommended LinkedIn privacy and safety settings to ensure your privacy and reduce the likelihood of becoming a scam victim or being hacked.

Center for Development of Security Excellence
CDSE

Suggested LinkedIn Privacy & Safety Settings

Privacy & Settings >>> ACCOUNT

For maximum security, while using LinkedIn, it is recommended to change the following settings:

Setting	Path to Get You There	Recommendation
Email Addresses	Privacy & Settings > Account > Basics	Only provide one email address to limit personal information available
Phone numbers	Privacy & Settings > Account > Basics	Provide a phone number to enable two-step verification
Change password	Privacy & Settings > Account > Basics	Follow secure password practices by changing your password once a month, using a mix of letters, numbers, and characters
Name, location, and industry	Privacy & Settings > Account > Basics	Please be aware of the information you are giving out
Where you're signed in	Privacy & Settings > Account > Basics	Review this setting frequently to help detect unauthorized access to your account
Third Party Apps	Privacy & Settings > Account > Third Parties	Review and limit third party apps
Twitter Settings	Privacy & Settings > Account > Third Parties	Do not allow data sharing with Twitter if you don't intend for your information to be shared through both services
WeChat Settings	Privacy & Settings > Account > Third Parties	Do not allow data sharing with WeChat, if possible
Try Premium for Free	Privacy & Settings > Account > Subscriptions	Your personal preference, but there may be a fee later
Closing your account	Privacy & Settings > Account > Subscriptions	Do this if you suspect your account or identity has been hacked or compromised

Privacy & Settings >>> COMMUNICATION

For maximum security, while using LinkedIn, it is recommended to change the following settings:

Setting	Path to Get You There	Recommendation
Email Frequency	Privacy & Settings > Communications > Basics	Set to "Off" to eliminate e-mails you receive from LinkedIn
Who can send you invitations	Privacy & Settings > Communications > Basics	Set to "Only people who know your email address or appear in your 'Imported contacts list'"
Messages from members	Privacy & Settings > Communications > Basics	Set to "Introductions Only" to limit messages you get from other members and to avoid phishing attempts
Group invitations	Privacy & Settings > Communications > Basics	Set to "No" unless you want to receive invitations to join groups. Be cautious of the groups you join
Group notifications	Privacy & Settings > Communications > Basics	Set to "No" so your network will not be notified when you join a group
Participate in research	Privacy & Settings > Communications > Basics	Set to "No" so you will be exempt from receiving invitations to participate in research
Partner InMail	Privacy & Settings > Communications > Basics	Set to "No" to eliminate unsolicited email from LinkedIn partner companies

Closing Your Account

If you no longer want your LinkedIn account, or suspect it has been hacked, you may close your account under: Account and Settings > Privacy & Settings > Account > Subscriptions

Privacy & Settings >>> PRIVACY

For maximum security, while using LinkedIn, it is recommended to change the following settings:

Setting	Path to Get You There	Recommendation
Two-Step Verification	Privacy & Settings > Account > Security	Set to "on" to verify login attempts and to sign out of other places you may be signed in
Sharing Profiles Edits	Privacy & Settings > Profiles > Privacy	Set to "No" to avoid notices to your network when you make a profile change
Notifying connections when you're in the news	Privacy & Settings > Account > Profile > Privacy	Set to "No" to prevent connections and followers from knowing when you are mentioned in the news
Who can see your connections	Privacy & Settings > Account > Profile > Privacy	Determine your privacy settings based on best security practices and your intended audience
Profile viewing options	Privacy & Settings > Account > Blocking and Hiding	Control what others see about you when you've viewed their profile
Followers	Privacy & Settings > Account > Blocking and Hiding	Control who can follow you and see your public updates

Sign Out

Always make sure to sign out when you are done, especially when using a shared computer.

Extracted from:

https://www.cdse.edu/Portals/124/Documents/jobajds/cyber/LinkedIn_Smartcard_Trifold.pdf?ver=usUI51YI2RgflFiErhxeRg%3d%3d

Twitter (20 minutes)

OVERVIEW

Find out how hackers can hack your Twitter account. You can be proactive to prevent from becoming a victim.

Center for Development of Security Excellence
CDSE

Twitter Smart Card
Security in an Insecure World

For optimum security, match your Twitter Privacy Settings to this example:

Access your Twitter account settings by clicking on your account picture.

Privacy

Photo tagging

☐ Allow anyone to tag me in photos
 ☒ Only allow people I follow to tag me in photos
 ☒ Do not allow anyone to tag me in photos

Tweet privacy

☒ Protect my Tweets

Tweet location

☒ Add a location to my Tweets

Discoverability

☒ Let others find me by my email address
 ☒ Let others find me by my phone number

Security

Login verification

☒ Don't verify login requests
 ☒ Send login verification requests to 1000-XXX-XXXX

☒ After you log in, Twitter will send a SMS message with a code that you'll need to access your account.
 ☒ Send login verification requests to the Twitter app.

☒ Approve requests with one tap when you are in login verification on Twitter for iPhone or Twitter for Android. Learn more

Password reset

☒ Require personal information to reset my password

Privacy

Personalization

☒ Tailor Twitter based on my recent website visits
 ☒ Tailor ads based on information shared by ad partners.

CDSE Recommendations

- Block "Direct Messages" from people you do not know.
- If you want to restrict your audience to specific user accounts, deny follow requests from people you do not know.
- De-select all Twitter tracking options.
- Establish and maintain connections with only people you know and trust; review your connections on a regular basis.
- Encourage your family and friends to take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Require login verification and personal information to reset your password.
- Set your account to "Private" to control who may follow (see), retweet (share), or quote (share with comment) your tweets.

Extracted from:

https://www.cdse.edu/Portals/124/Documents/jobajds/cyber/cyb-twitter-smartcard.pdf?ver=r6-OLp-b8A5YA_rQ9sI2AQ%3d%3d

Page | 28

Cybersecurity Awareness Training
Facilitator's Guide

KEY TAKEAWAYS

- Apply the recommended privacy settings as described by the Center for Development of Security Excellence.

Learning Checkpoint #2 (30 minutes)

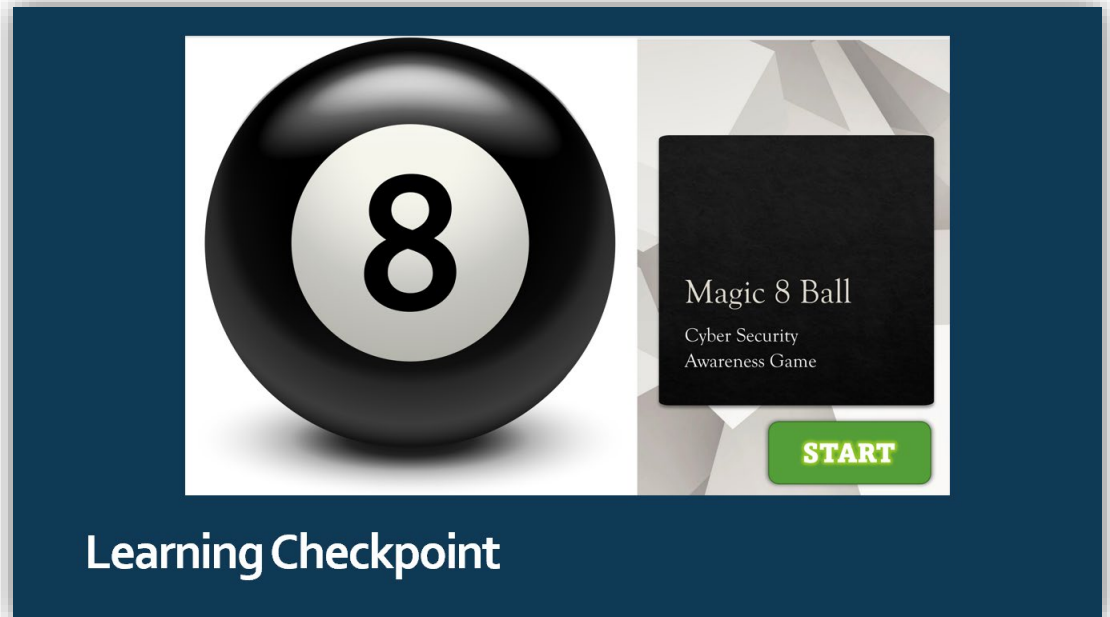
Description

Option 1: Magic 8 Ball Game
Option 2: Cybersecurity Trivia
Option 3: Cybersecurity Crossword Puzzle

Materials

- ☐ Facilitator presentation & notes
- ☐ Option 1: Magic 8 Ball PowerPoint file
- ☐ Option 2:
<https://securityawareness.usalearning.gov/cdse/multimedia/games/cybertrivia/index.html#>
- ☐ Option 3:
<https://securityawareness.usalearning.gov/cdse/multimedia/games/cybersecurity-crossword/index.html>

OPTION 1



FACILITATOR NOTES

This activity runs as part of the PowerPoint presentation. The questions can be changed, more questions can be added, other questions can be deleted; instructions to do this are included within the slide presentation.

This game is meant as a review of the concepts discussed thus far in the training.

- The facilitator will ask the Magic 8 ball the question.
- Participants respond with what they think is the answer.
- Clicking on the [ASK] button reveals the correct answer.
- Clicking again on the [NEXT] button reveals the next question to be asked of the Magic 8 Ball.
- Based on the response from the participants, this gives the facilitator the opportunity to revisit topics that may not be clear.

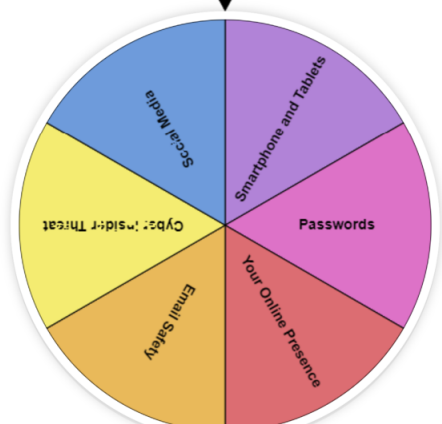
OPTION 2

Learning Checkpoint Cybersecurity Trivia

Open a browser and go to:
<https://securityawareness.usalearning.gov/cdse/multimedia/games/cybertrivia/index.html#>

Cybersecurity Trivia Twirl

SPIN THE WHEEL



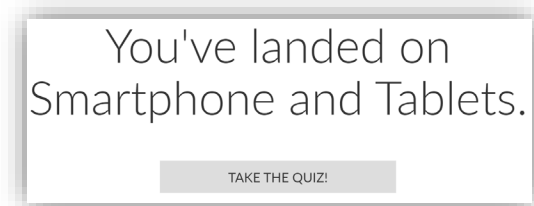
FACILITATOR NOTES

The link on the slide

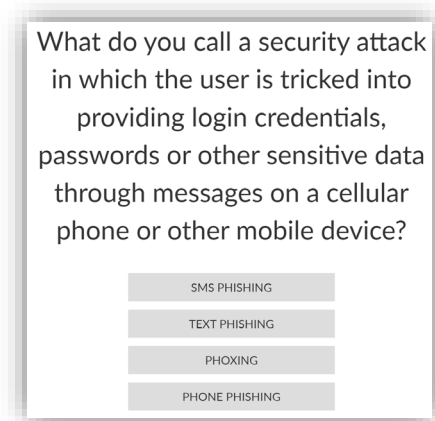
<https://securityawareness.usalearning.gov/cdse/multimedia/games/cybertrivia/index.html#> will take the facilitator to the website where the Trivia Wheel is located.

This game is meant as a review of the concepts discussed thus far in the training.

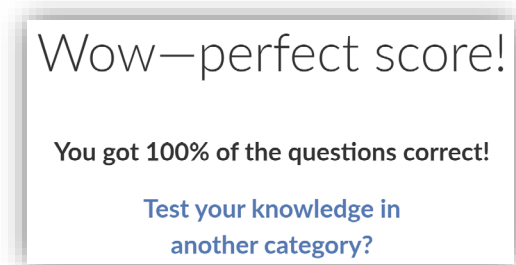
- Click on the [SPIN THE WHEEL] button.
- The wheel will spin and stop on a category (see example):



- Click on the [TAKE THE QUIZ!] button.
- The quiz is five questions. Each question provides choices for an answer:



- Ask the participants what they think the answer is and then click on the button that they think is the answer.
- After going through all five questions a score is given:



- The facilitator can then click on the link to spin the wheel again to try another category.

OPTION 3

Learning Checkpoint Cybersecurity Online Crossword Puzzle

Open a browser and go to:
<https://securityawareness.usalearning.gov/cdse/multimedia/games/cybersecurity-crossword/index.html>



FACILITATOR NOTES

The link on the slide
<https://securityawareness.usalearning.gov/cdse/multimedia/games/cybersecurity-crossword/index.html> will take the facilitator or participant to the website where the crossword puzzle is located.

This game is meant as a review of the concepts discussed thus far in the training. It can be run as a discussion or an individual activity.

**BREAK
(15 Minutes)**

Stay cyber-safe when working remotely (30 minutes)

Description Tips while working (or playing) online.

Sections Tips for being cyber-safe working remotely (30 mins.)

Materials

- ☐ Facilitator presentation & notes

How to Stay Safe Online While Working from Home

<https://youtu.be/DRTWegPpM2s>

VIDEO – 1 minute, 39 seconds





Tips for working from home

- Create your own office space and keep others in the family from using it.
- Don't leave confidential paperwork laying around.
- Lock your computer when not in your working area. [WINDOWS + L] key
- Don't use your personal email to send yourself work documents.
- Use only company-approved applications and devices when communicating with your co-workers and business contacts (e.g. Teams, work email account, company laptop or phone).
- If you get a request for confidential information from a co-worker, call or contact your co-worker to verify they made the request.
- Have Siri turned off and put Alexa and Google Home devices in another room to make sure they aren't listening.

Adapted from: <https://www.wizer-training.com/guides/work-from-home>





Tips for working from home (continued)

- Do not share company devices with family members.
- Don't save your passwords to your browser!
- Use long pass phrases for your passwords and make each account with a different pass phrase.
- Don't use your work computer for personal activities.
- Whenever possible use a hard-wired network connection instead of a wireless one.
- Always apply the security patches sent to your company-issued devices (e.g. computer, tablet, and/or phone).
- Make sure you are backing up your data using the approved method provided by the company.

Adapted from: <https://www.wizer-training.com/guides/work-from-home>




Adapted from: <https://www.wizer-training.com/guides/work-from-home>

FACILITATOR NOTES

Use the bullet points to guide a discussion on the tips for working from home.

Do the participants have any others they would like to share?

Closing Remarks (5 minutes)

Description Thank attendees for participating and direct them to the additional resources.



RESOURCES

- Bitdefender. (2022). *Bitdefender Premium VPN*. Bitdefender Premium VPN. Retrieved May 4, 2022, from <https://www.bitdefender.com/solutions/vpn.html>
- Center for Development of Security Excellence. (2016, April). *Facebook Smart Card* [PDF Document]. <https://www.cdse.edu/Portals/124/Documents/jobbaid/cyber/cyb-facebook-smartcard.pdf?ver=9evqdckfQgOngmwL7OHMOA%3d%3d>
- Center for Development of Security Excellence. (2016, June). *Twitter Smart Card* [PDF Document]. https://www.cdse.edu/Portals/124/Documents/jobbaid/cyber/cyb-twitter-smartcard.pdf?ver=r6-OLp-b8A5YA_rQ9sl2AQ%3d%3d
- Center for Development of Security Excellence. (2016, September). *LinkedIn Social Media Smart Card* [PDF Document]. https://www.cdse.edu/Portals/124/Documents/jobbaid/cyber/LinkedIn_Smartcard_Tifold.pdf?ver=usUI51YI2RgflFiErhxeRg%3d%3d
- Cofense. (2022, April 27). *Phishing Database: Real Email Phishing Attack Examples & Threats*. Retrieved April 27, 2022, from <https://cofense.com/real-phishing-examples-and-threats/>
- Cybersecurity. (2022). Center for Development of Security Excellence. Retrieved April 26, 2022, from <https://www.cdse.edu/Training/Cybersecurity/>
- Federal Bureau of Investigation. (n.d.). *Internet Social Networking Risks* [PDF Document]. <https://www.fbi.gov/file-repository/internet-social-networking-risks-1.pdf>
- Federal Trade Commission. (n.d.). *Cybersecurity Quizzes*. Retrieved April 30, 2022, from <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz>
- Federal Trade Commission. (n.d.). *Report to help fight fraud!* Retrieved May 4, 2022, from <https://reportfraud.ftc.gov/#/>
- Federal Trade Commission. (n.d.). *What To Do Right Away*. IdentityTheft.gov. Retrieved May 4, 2022, from <https://www.identitytheft.gov/#/Steps>
- Field Offices - FBI*. (n.d.). Retrieved May 4, 2022, from <https://www.fbi.gov/contact-us/field-offices>

IDG TECHtalk. (2019, August 28). *What is phishing? Learn how this attack works* [Video].

<https://www.youtube.com/watch?v=Y7zNIEMDml4&list=PPSV>

Infosec. (2020, December 4). *How to carry out a watering hole attack* [Video].

https://www.youtube.com/watch?v=nNzUg_gW1tl

Internet Crime Complaint Center. (n.d.). *Internet Crime Complaint Center*. Retrieved May 4, 2022, from

<https://www.ic3.gov/>

Jones, T. (2022, March 25). The 12 Latest Types of Social Engineering Attacks (2022). *Aura*.

<https://www.aura.com/learn/types-of-social-engineering-attacks>

KnowBe4. (2022). *Top Clicked Phishing Tests* [Infographic; PDF format].

<https://www.knowbe4.com/hubfs/Q1-2022.pdf>

McAfee Cloud BU. (2015, August 7). How to Create a Strong Password You Actually Remember.

<https://www.mcafee.com/blogs/enterprise/cloud-security/how-to-create-a-strong-password-you-actually-remember/>

Miessler, D. (2019, December 17). The Internet, the Deep Web, and the Dark Web. *Daniel Miessler*.

<https://danielmiessler.com/study/internet-deep-dark-web/>

Nadeem, M. S. (2021, December 2). How to keep your private email account secure.

<https://blog.mailfence.com/keep-your-private-email-account-secure/>

No-Nonsense Security Awareness. (n.d.). Retrieved April 26, 2022, from [https://www.wizer-](https://www.wizer-training.com/)

[training.com/](https://www.wizer-training.com/)

NortonLifeLock Inc. (2022). *Norton Secure VPN*. Retrieved May 4, 2022, from

<https://us.norton.com/products/norton-secure-vpn>

Phishing Examples. (2022). Phishing.org. Retrieved April 26, 2022, from

<https://www.phishing.org/phishing-examples?hsLang=en>

Richter, F. (2020, August 11). The Most Impersonated Brands in Phishing Scams. *Statistica*.

<https://www.statista.com/chart/22528/most-impersonated-brands-in-phishing-attacks/>

Security and Microsoft Teams. (2022, April 12). [https://docs.microsoft.com/en-](https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide)

[us/microsoftteams/teams-security-guide](https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide)

Select E-Learning Awareness Courses for DOD and Industry. (2022). Security Awareness Hub. Retrieved April 26, 2022, from <https://securityawareness.usalearning.gov>

Singh, I. (2017, November 7). Safe Computing Checklist | A beginner's practical guide to a secure computer. <https://medium.com/@ishmeet/safe-computing-checklist-a-practical-guide-to-secure-your-computer-bfb7582b5f5d>

Southside Bank. (2019, September 17). *Business Email Compromise Scams Simplified* [Video]. <https://www.youtube.com/watch?v=h3ipCndIq0>

Stack, B. (2017, December 6). Here's How Much Your Personal Information Is Selling for on the Dark Web. <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

StaySafeOnline.org. (2019, November 5). *Security Awareness Episode 1: Passwords* [Video]. <https://www.youtube.com/watch?v=0Wd3JoUHXno>

StaySafeOnline.org. (2020, June 29). *Security Awareness Episode 5: Removable Media* [Video]. <https://www.youtube.com/watch?v=FRxrHduwPjY>

StaySafeOnline.org. (2020, September 9). *Security Awareness Episode 6: Vishing* [Video]. <https://www.youtube.com/watch?v=Hc01oZPvByg>

Stop Phishing Attacks From Hitting Your Organization. (2022). Phishing.org. Retrieved April 26, 2022, from <https://www.phishing.org>

Techlore. (2020, August 1). *Become Anonymous: The Ultimate Guide To Privacy, Security, & Anonymity* [Video]. <https://www.youtube.com/watch?v=a1i-3xwcSGA>

U.S. Department of Homeland Security. (202). *Stay #CyberAware While On the Go – Safety Tips for Mobile Devices.* Stop Think Connect. Retrieved May 4, 2022, from <https://stopthinkconnect.org/resources/preview/tip-sheet-stay-cyberaware-while-on-the-go-safety-tips-for-mobile-devices>

U.S. Department of Justice. (n.d.). *FBI - Tips.* Retrieved May 4, 2022, from <https://tips.fbi.gov/>

Wizer. (n.d.). *Zoom: Protecting Your Meeting Security Guide* [PDF Document]. [https://f.hubspotusercontent40.net/hubfs/5120248/Downloadable%20Content%20Offers/Kids%20Campaign%20\(Jun%2010\)/Zoom%20-%20Security%20Guide.pdf](https://f.hubspotusercontent40.net/hubfs/5120248/Downloadable%20Content%20Offers/Kids%20Campaign%20(Jun%2010)/Zoom%20-%20Security%20Guide.pdf)

Wizer Training. (n.d.). *Work From Home Cyber Security Employee Guide* [PDF Document].

<https://f.hubspotusercontent40.net/hubfs/5120248/flipbook-1.pdf>