

Cybersecurity Awareness Training Participant Packet



Cybersecurity Awareness Training

About this Training

This training will cover topics such as understanding social engineering attacks and scams, social engineering prevention strategies, social media compromise and safety, and tips for staying safe online while working remotely.

Cybersecurity awareness is about making deliberate decisions to protect the confidentiality, integrity, and availability of information whether it is for business or personal reasons. It is important to understand the implications of using the internet for our everyday work and personal online activities. Unlike other training opportunities, this one can benefit you on both a personal and professional level.

Social engineering is the number one problem when it comes to protecting our networks and data. Social engineering has to do with the variety of methods used to manipulate a human being to give out personal or confidential information. This information is then used in conducting scams, breaching networks, ransomware attacks, personal identity theft, disintegrating goodwill between companies, and more. The consequences of not keeping up or following best practices for cybersecurity are simply too great to ignore.

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 or prevent them.
- Know what it means to be safe when engaging in social media.
- Understand how to stay protected while working (and playing) online.

ADDITIONAL RESOURCES

Description	Link
Stay Safe Online website	https://staysafeonline.org/
In the case of a ransomware attack contact your local FBI office	https://www.fbi.gov/contact-us/field-offices
Submit a tip to the FBI online	https://tips.fbi.gov/
File a report with the FBI's Internet Crime Complaint Center (IC3)	https://www.ic3.gov/
First steps in reporting identity theft	https://www.identitytheft.gov/#/Steps
Phishing examples	https://www.phishing.org/phishing-examples
Norton VPN software	https://us.norton.com/products/norton-secure-vpn
BitDefender VPN software	https://www.bitdefender.com/solutions/vpn.html
Facebook safety card	https://www.cdse.edu/Portals/124/Documents/jobaid/cyber/cyb-facebook-smartcard.pdf?ver=9evqdckfQqOngmwL7OHMOA%3d%3d
LinkedIn safety card	https://www.cdse.edu/Portals/124/Documents/jobaid/cyber/LinkedIn_Smartcard_Tifold.pdf?ver=usUI51YI2RgflFiErhxeRg%3d%3d
Twitter safety card	https://www.cdse.edu/Portals/124/Documents/jobaid/cyber/cyb-twitter-smartcard.pdf?ver=r6-OLp-b8A5YA_rQ9sl2AQ%3d%3d
Report fraud to the Federal Trade Commission	https://reportfraud.ftc.gov/#/
Mobile device safety tips	https://stopthinkconnect.org/resources/preview/tip-sheet-stay-cyberaware-while-on-the-go-safety-tips-for-mobile-devices
Internet Social Networking Risks	https://www.fbi.gov/file-repository/internet-social-networking-risks-1.pdf/view
Zoom conferencing safety tips	https://f.hubspotusercontent40.net/hubfs/5120248/Downloadable%20Content%20Offers/Kids%20Campaign%20(Jun%2010)/Zoom%20-%20Security%20Guide.pdf
Microsoft Teams Security Guide	https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide
National Cyber Security Alliance video "Security Awareness Episode 1: Passwords" Video	https://youtu.be/0Wd3JoUHXno
National Cyber Security Alliance video: "Security Awareness Episode 5: Removable Media" Video	https://youtu.be/FRxrHduwPjY
National Cyber Security Alliance video: "Security Awareness Episode 6: Vishing" Video	https://youtu.be/Hc01oZPvByg
"Becoming Anonymous – The Ultimate Guide to Security, Privacy & Anonymity" Video	https://www.youtube.com/watch?v=a1i-3xwcSGA

