CONARD HOUSE
EMPOWERING PEOPLE • RESTORING HOPE

SFHSA
Department of Disability and Aging Services

Introduction to Cybersecurity & Internet Safety - Week 2

This program serving the community is funded by the City of San Francisco's Department of Disability and Aging Services.

What is Phishing?

Phishing is a type of cyberattack where scammers trick people into revealing sensitive information—like passwords, credit card numbers, or Social Security details—by pretending to be a trustworthy source.

Phishing Sample Email

IRS

Third Round of Economic Impact Payments Status Available.

Dear Tax Payer, We hope this message finds you well. We are writing to inform you abount an important matter regarding your recent tax return filing.

Our record indicate that we have received your tax return for the fiscal year 2023. However, upon review, we have identified certain inconsistencies or missing information that require your attention and clarification.

You will receive a tax refund of $497.00 , We will process this amount once you have submitted the document we need for the steps to claim your tax refund.

Date : Monday, July 10, 2023
Sender : INTERNAL REVENUE SERVICE

To expedite the process and avoid further delays or penalties, we advise you to confirm the required document now .

For your convenience, we recommend not using a prepaid card, because sending funds does not support this card

COMPLETE MY INFORMATION

Questions? We're here to help. Call us at 1-800-659-2955 | TTY/TDD: 1-800-977-8339
Office of Disaster Assistance U.S. Small Business Administration.

Take a look at this email and the one on the next page.

Who is this message from, and what is it trying to convince you of?

What action do you think the reader will take?

Image from us.norton.com/blog/online-scams/phishing-email-examples

Phishing Sample Email

Unusual sign-in activity

We detected something unusual about a recent sign-in to the Microsoft account du*****@hotmail.com.

Sign-in details

Country/region: Japan

IP address: 207.148.101.217

Date: 9/20/2018 9:46 AM (GMT)

Platform: Windows

Browser: Internet Explorer

Please go to your recent activity page to let us know whether or not this was you. If this wasn't you, we'll help you secure your account. If this was you, we'll trust similar activity in the future.

Review recent activity

To opt out or change where you receive security notifications, click here.

Thanks,
The Microsoft account team

What tactic is the author of this message using here to elicit a reaction?

Why Are Both Emails Phishing?

1. Both messages claim to be from important or well-known agencies or companies.
2. Both messages do not refer to you by name - they have either a generic greeting or no greeting at all.
3. Both messages are trying to appeal to your emotions. The first one offers a happy “promise” of money, while the second one tries to scare you into thinking something is wrong.
4. Both messages convince you to act urgently so you don’t lose your money or so you maintain the security of your account.
5. Both messages have grammar or spelling mistakes, though the first one has more obvious errors.
6. Both have an external link where you can click to input either personal or account information.
7. The first email includes an authentic-looking logo.
8. If you click on the links and input your personal or account information, you are giving cyber criminals or hackers clear access to your identity, privacy, and finances.

Other Signs of Phishing

1. Urgent call to action or threats
2. First time, infrequent senders, or senders marked [External]
3. Spelling and bad grammar
4. Generic greetings
5. Mismatched email domains - If the email claims to be from a reputable company, like Microsoft or your bank, but the email is being sent from another email domain like Gmail.com, or microsoftsupport.ru it's probably a scam.
6. Your email provider shows you a banner that says we could not verify the sender
7. Suspicious links or unexpected attachments

support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

Protection from Phishing

1. Think Before You Click - Don't click on links or download attachments from unknown or suspicious emails, texts, or messages.

2. Verify the Sender
Check the sender's email address carefully. If in doubt, contact the company directly using a trusted method.

3. Use Multi-Factor Authentication (MFA)
Add an extra layer of security to your accounts so even if your password is stolen, hackers can't get in.

4. Keep Software Updated
Regular updates fix security flaws that phishing attacks may exploit.

5. Install Anti-Phishing Tools
Use browser extensions or antivirus software that detect and block phishing attempts (e.g., Norton, Bitdefender, Microsoft Defender SmartScreen).

6. Educate Yourself and Others
Learn to recognize phishing tactics and share that knowledge with friends, family, or coworkers.

7. Report Suspicious Messages
Most email platforms let you report phishing. Doing so helps protect others too.

support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

What To Do If You've Been Phished?

- While it's fresh in your mind write down as many details of the attack as you can recall. In particular try to note any information such as usernames, account numbers, or passwords you may have shared, and where the attack happened such as in Teams, or Outlook.
- Immediately change the passwords on all affected accounts, and anywhere else that you might use the same password. While you're changing passwords you should create unique passwords for each account, and you might want to see Create and use strong passwords.
- Confirm that you have multifactor authentication (also known as two-step verification) turned on for every account you can. See What is: Multifactor authentication
- If this attack affects your work or school accounts, you should notify the IT support folks at your work or school of the possible attack. If you shared information about your credit cards or bank accounts, you may want to contact those companies as well to alert them to possible fraud.
- If you've lost money, or been the victim of identity theft, don't hesitate, report it to local law enforcement.

support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

Spam Texts

In 2024, the Federal Trade Commission reported that Americans lost roughly $470 million from scam texts. Spam texts, also known as “smishing,” are a growing issue, and many people become victims because they aren’t aware of the methods scammers use to steal their information. Knowing spam text message examples can help you protect yourself and be aware of the various types of scams.

1. Deliveries

These scams impersonate delivery services, claiming an issue with your package to trick you into providing information or paying a fee.

Example text: “USPS: Your package is pending delivery due to an unpaid shipping fee. Please update your information here to avoid return: [suspicious link]”

www.pandasecurity.com/en/mediacenter/spam-text-message-examples/

Spam Texts

2. Free Gift Cards or Prizes

These enticing messages promise valuable rewards like gift cards or prizes to lure you into clicking on spoofed or malicious website links or providing personal details.

Example text: "Congratulations! You've won a $100 Amazon gift card! Click here to claim your prize now: [phishing link]"

3. Job Offers

Be wary of unsolicited text messages offering lucrative job opportunities, especially those that seem too good to be true or require an upfront fee.

Example text: "URGENT HIRING! Earn $500/day working from home. No experience needed. Apply here: [scam job application link]"

www.pandasecurity.com/en/mediacenter/spam-text-message-examples/

Spam Texts

4. Texts From Government Agencies
Impersonating government agencies like the IRS or Social Security Administration, these texts often threaten legal action or promise benefits to scare you into providing personal information or money.
Example text: "IRS Notice: You have an outstanding tax issue. Immediate action is required to avoid penalties. Visit: [fake IRS website link]"

5. Romance/Friend Text
This is one of the popular SMS scams that is difficult to identify because they are intentionally made to seem like real texts that could have accidentally been sent to the wrong person.
Example text: "Hey there. Jenny gave me your number, and I'm in SF. Want to go to a local restaurant sometime?"

www.pandasecurity.com/en/mediacenter/spam-text-message-examples/

How To Identify Spam Texts

- The message has no relevance to you.
- The message conveys a sense of urgency.
- The message is from an unfamiliar phone number.
- The message contains misspellings and poor grammar.
- The message has a suspicious link.

To further protect yourself, please take these important steps:

- Block the spam text number to prevent future messages, then delete the text to avoid clicking the links later.
- **Never respond** to unsolicited texts or click on links in a text from an unknown or suspicious sender.
- **Never share** any personal or financial information with an unknown sender.
- Be cautious about where you share your cell phone number or other personal information.
- Regularly update your phone's security settings.

www.pandasecurity.com/en/mediacenter/spam-text-message-examples/

QR Codes

QR Code stands for “Quick Response Code.” It’s a type of barcode designed for rapid readability and high storage capacity. QR codes have evolved into a widely used tool in various sectors. Their unique pattern of black squares arranged on a white background encodes information that, when scanned, provides instant access to data, websites, or other digital resources. QR codes, easily recognized as those square-shaped barcodes, are designed to store information in a way that digital devices can quickly read.

Unfortunately, QR codes can also be a cybersecurity risk, if one isn’t careful.

www.malwarebytes.com/cybersecurity/basics/what-is-a-qr-code

QR Code Scams

Hackers may manipulate QR codes to conduct malicious activities in two primary ways:

- **Malicious URL (Web Address) Embedding -** By encoding a harmful URL into a QR code, attackers can lead individuals to download malware or unwanted software. Once scanned, these QR codes can initiate the download and installation of malware, putting personal data at risk.
- **Phishing Expeditions -** Similar to malicious URL embedding, hackers can also direct users to phishing websites through a QR code. These websites, often masquerading as legitimate sites, aim to trick individuals into entering sensitive information, such as login credentials or financial data, thereby compromising their security.

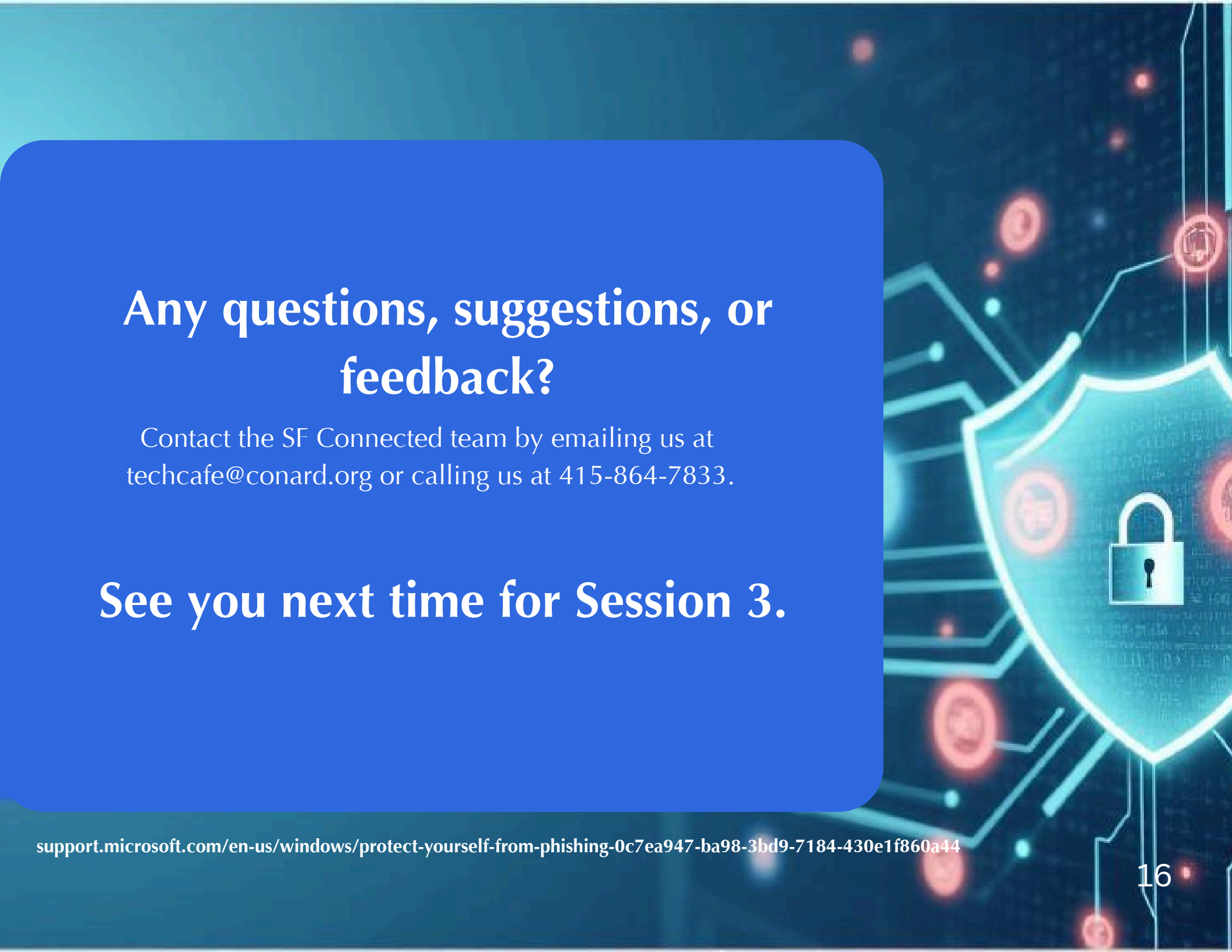
www.malwarebytes.com/cybersecurity/basics/what-is-a-qr-code

QR Code Safety

1. **Verify Before Scanning:** Always confirm the source of a QR code before scanning. If it's from an unknown or suspicious source, avoid scanning it.
2. **Use Secure QR Code Scanners:** Some QR code scanner apps offer additional security features, like checking the URL for known security threats before opening it.
3. **Stay Informed:** Regularly update yourself on the latest cybersecurity practices and educate others about the risks associated with QR codes.

By understanding these risks and taking the necessary precautions, users can significantly mitigate the potential threats posed by compromised QR codes.

www.malwarebytes.com/cybersecurity/basics/what-is-a-qr-code



Any questions, suggestions, or feedback?

Contact the SF Connected team by emailing us at techcafe@conard.org or calling us at 415-864-7833.

See you next time for Session 3.

support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44