PHISHING AWARENESS TRAINING

PRESENTATION BY RICHARD KUSI

CA/AG1/30978

2nd August,2024

OUTLINE

- RECOGNIZING PHISHING EMAILS
- RECOGNIZING PHISHING WEBSITES
- SOCIAL ENGINEERING TACTICS
- COMMON SOCIAL ENGINEERING TECHNIQUES
- BEST PRACTICES TO AVOID PHISHING ATTACKS
- CASE STUDY
- CONCLUSION
- REFERENCES
- QUESTIONS AND ANSWERS

RECOGNIZING AND AVOIDING PHISHING ATTACKS

OBJECTIVES

- UNDERSTAND WHAT PHISHING IS AND ITS VARIOUS FORMS.
- RECOGNIZE COMMON SIGNS OF PHISHING EMAILS AND WEBSITES.
- LEARN ABOUT SOCIAL ENGINEERING TACTICS USED IN PHISHING.
- IMPLEMENT BEST PRACTICES TO AVOID PHISHING ATTACKS.

INTRODUCTION TO PHISHING

What is Phishing?

Phishing is a type of cyber attack, whereby an attacker makes a fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity. These attacks are often conducted through emails,websites, and other communication channels.

TYPES OF PHISHING ATTACKS

- **Email Phishing**: Fraudulent emails that appear to be from legitimate sources.
- **Spear Phishing**: Targeted phishing attacks directed at specific individuals or organizations.
- **Whaling**: Phishing attacks aimed at senior executives and other high-profile targets.
- **Smishing**: Phishing attacks conducted via SMS messages.
- **Vishing**: Phishing attacks conducted via voice calls.

RECOGNIZING PHISHING EMAILS

Red Flags in Phishing Emails…

- Generic greetings (e.g., 'Dear Customer').
- Suspicious sender email addresses.
- Urgent or threatening language.
- Unusual requests for personal information.
- Unusual attachments or links.

EXAMPLE OF A PHISHING EMAIL

🏆 CONGRATS AYOMAX91 🏆 We Have Added 💲 52.000,00 USD To Your Account ⚠️ Please confirm now or you lose access " in 72h"⚠️Sun, 13 Mar 2022 20:54:40 -0400

BitCoin-Code figgzfxxvmcsjcencdfdtq...@jwapdztfxxei.org.uk via cofeci.gov.br
to

Fake email address

Mar 14, 2022, 1:54 AM (5 days ago)

Why is this message in spam? It seems to be an auto-reply to a message that pretended to be sent from your email address.

Report not spam Report phishing

Your-Funds | Your account | Bitcoin.com

Transaction confirmation

Order n° 502-20201222 -05680829238

Congratulations Dear Ayomax91,

You have successfully received **$ 52.000,00 USD** into your account , your Transaction n°502-20201222-05680829238

➢ACCOUNT INFORMATION:

➥ E-mail:
ayomax91@gmail.com

➥ Name :
Ayomax91

➥ Account expires:
in 72 Hours

the Transaction is delivered to :
Ayomax91

Suspicious link to claim prize

Details of the transaction

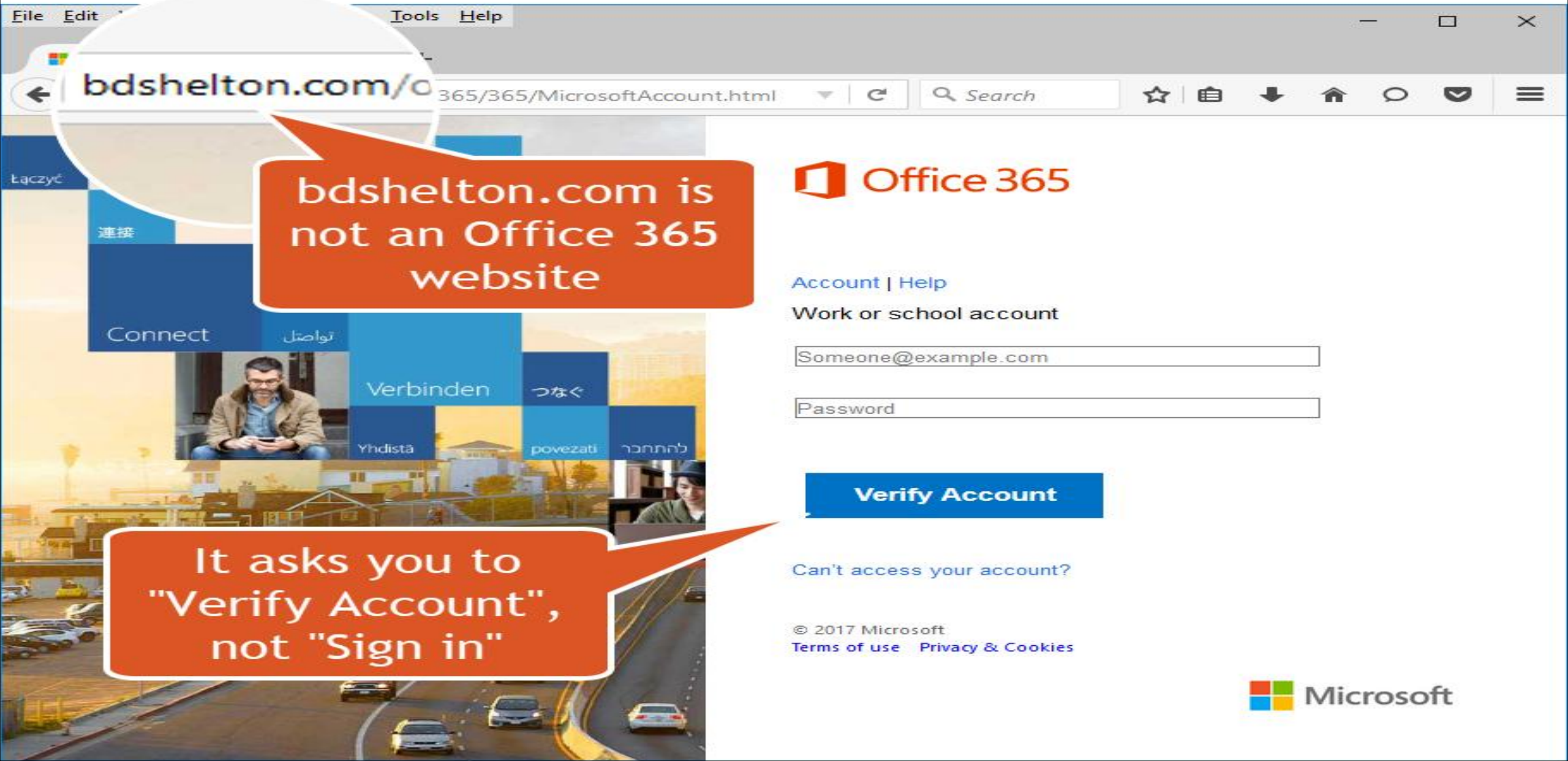
502-20201222-05680829238

RECOGNIZING PHISHING WEBSITES

Identifying Fake Websites:

- Check the URL for slight misspellings or unusual domains.
- Look for HTTPS and a padlock icon.
- Be wary of pop-ups asking for personal information.
- Check for poor design or language errors.

EXAMPLE OF A PHISHING WEBSITE…



SOCIAL ENGINEERING TACTICS

What Is Social Engineering?

Social engineering is the psychological manipulation of individuals into performing actions or divulging confidential information. A common example is Phishing.

COMMON SOCIAL ENGINEERING TECHNIQUES

- **Pretexting**: Creating a fabricated scenario or lying to steal personal information.
- **Baiting**: Offering something enticing to get personal information.
- **Quid Pro Quo**: Offering a service in exchange for information.
- **Tailgating**: Following someone into a restricted area to gain access.

BEST PRACTICES TO AVOID PHISHING ATTACKS

Email Security Tips

- Always verify the sender's email address.
- Question the authenticity of unexpected emails.
- Avoid clicking on links in unsolicited emails.
- Enable MFA for an extra layer of security.

Web Security Tips

- Always check the URL before entering sensitive information.
- Use bookmarks for frequently visited websites to avoid typing errors.
- Use reputable security software to detect and block phishing websites.

CONT'D.....

BEST PRACTICES TO AVOID PHISHING ATTACKS

General Security Tips

1. Stay informed about the latest phishing tactics.

2. Report suspicious emails and websites to your IT department or relevant authority.

3.Keep your software and systems updated to protect against vulnerabilities.

CONT'D.....

CASE STUDY

Real-life Example Of A Phishing Attack:

Target Data Breach (2013)

In 2013, cybercriminals used a phishing email to gain access to Target's network through a third-party vendor. The attackers installed malware on Target's point-of-sale systems, compromising the credit and debit card information of approximately 40 million customers and personal information of about 70 million more.

Impact

- Organization: $18.5 million in settlements, reputational damage, and enhanced security costs.
- Individuals: 40 million card details and 70 million personal records compromised.

CASE STUDY

Lessons Learned and Preventative Measures

- Improved network segmentation and monitoring.
- Tighter access controls for third-party vendors.
- Better cybersecurity training to recognize phishing.
- Continuous security assessments.

CONT'D...

CONCLUSION

Phishing attacks are a significant threat, but by staying vigilant and following best practices, you can protect yourself and your organization. Always be cautious, verify suspicious communications, and report any phishing attempts to help keep everyone safe.

Key Takeaways:

- Always be vigilant and skeptical of unexpected communications.
- Educate yourself and others on recognizing phishing attempts.
- Implement security measures to protect against phishing attacks.

RESOURCES

- https://images.app.goo.gl/PhRNqaVC3kKhjQsQ9
- https://youtu.be/zflsg6TRuos?si=nJn1dQmFQchHNvWo
- https://www.msvu.ca/campus-life/campus-services/it-services/it-security/phishing/phishing-login-form-examples/
- https://images.app.goo.gl/PhRNqaVC3kKhjQsQ9

QUESTIONS AND ANSWERS