Can you spot a Phish?

By Jody Jacobs
National Institute of Standards and Technology

26 September 2023
BLUE CYBER EDUCATION SERIES
Can you spot a phish?
Disclaimer

Throughout the presentation, certain commercial companies or products may be identified to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the companies or products identified are necessarily the best available for the purpose.
Presentation Overview

• Who we are

• Phishing threat landscape

• Our research

• How to spot a phish
Championing the Human in I.T.
Phishing Threat Landscape
Phishing Landscape

- Phishing attacks have quintupled since 2020.¹
- Breaches involved the human element in 2021.³
- 5x
- 82% Reported spear phishing attacks in 2022.⁴
- $10.2B Victim losses in 2022.²
Phishing Defense

Technology
- Filtering
- DMARC, DKIM
- AI & ML
- Multi-factor authentication

Process
- Identify vulnerabilities
- Limiting publicly available information
- Awareness training
- Easy and clear reporting mechanism
- Meaningful metrics

People
- End users
- IT security staff
- Leadership
Phishing Defense

Technology
• Filtering
• DMARC, DKIM
• AI & ML
• Multi-factor authentication

Process
• Identify vulnerabilities
• Limiting publicly available information
• Awareness training
• Easy and clear reporting mechanism
• Meaningful metrics

People
• End users
• IT security staff
• Leadership
Phishing Awareness Training

Training in Practice

- Simulated phishing emails
- Gamify phishing
  - e.g., phish hunting badges, shark awards
- Staff Profiles

Common Metrics and Behaviors

- Click rates
- Reporting rates
- Repeat clickers
- Protective stewards\(^5\)
OUR RESEARCH
Our Research – Phishing Awareness Study

Phishing scams continue…

It’s a phish.

It’s a scam!

It’s a phish.

Alrighty.

Some users click, some don’t. Why?
Our Research – Phishing Awareness Study

Alignment vs. misalignment with expectations and external events

Concern over consequences

Email premise

Interpreting cues

Consequences

Reality checking

Reality-checking strategies

Compelling vs. suspicious cues

User Context
Phish Scale

Premise Alignment

Cues

HIGH

MEDIUM

LOW

FEW  SOME  MANY

VERY DIFFICULT

MODERATELY DIFFICULT

LEAST DIFFICULT
Our Research

HOW TO SPOT A PHISH
How to Spot a Phish – Investigate Email

Check if the email is a threat:

- Does it contain a link?
- Does it contain an attachment?
- Does it request information?

No Yes
Phish Scale – Cues

Always check for spelling mistakes

NOW

Click here

Winner!

Congratulations you are owed

McDowell's

How to Spot a Phish – Where to Find Cues

FROM: Jane Doe (Fed) <jane.doe@nist.gov>

Mon 3/27/2021 12:55 PM

To: Doe, John (Fed)

Subject: Interesting data for the presentation

From: Jane Doe (Fed) <jane.doe@nist.gov>

Hi John,

Here’s a file I found with really interesting data. Check it out.

Regards,

Jane

Jane.Doe@nist.gov

NOTICE: This message is intended solely for the individual to whom this e-mail is addressed. The contents of this message and any files transmitted are confidential. Notify the sender immediately if you have received this e-mail in error.
How to Spot a Phish – What Cues to Look for

• 5 Types of Cues
  • Errors
  • Technical indicators
  • Visual presentation indicators
  • Language and content
  • Common tactics
How to Spot a Phish – What Cues to Look for

• 5 Types of Cues

  • Errors

  • Technical indicators

  • Visual presentation indicators

  • Language and content

  • Common tactics

From: Order Confirmation [mailto:no-reply@discontcomputers.com]
Sent: Thursday, December 01, 2016 11:50 PM
To: Doe, Jane (Fed) <jane.doe@nist.gov>
Subject: Jane DoeYour order has been processed
How to Spot a Phish – What Cues to Look for

• 5 Types of Cues

  • Errors
  
  • Technical indicators
  
  • Visual presentation indicators
  
  • Language and content
  
  • Common tactics

From: Preston, Jill (Fed) [mailto:jill.preston@nist.gov]
Sent: Friday, August 05, 2016 12:03 PM
To: Doe, Jane (Fed) <jane.doe@nist.gov>
Subject: Unpaid invoice #4806
How to Spot a Phish – What Cues to Look for

• 5 Types of Cues

  • Errors
  • Technical indicators
  • Visual presentation indicators
  • Language and content
  • Common tactics
How to Spot a Phish – What Cues to Look for

• 5 Types of Cues
  • Errors
  • Technical indicators
  • Visual presentation indicators
  • Language and content
  • Common tactics

A secret admirer wished you a Happy Valentine’s Day!

Some of you may have heard about our employee greeting cards that can be used to acknowledge fellow employees.

Click on the link below to view yours.

Your Card is Waiting

If you are having trouble viewing the e-card please click here.

Would you like to send an e-card? Visit our site.

Making someone’s day, one e-card at a time...
How to Spot a Phish – What Cues to Look for

- 5 Types of Cues
  - Errors
  - Technical indicators
  - Visual presentation indicators
  - Language and content
  - Common tactics

From: Jacob, Jodi [mailto:Jodi.Jacob@gmail.com]
Sent: Friday, August 05, 2016 12:03 PM
To: Doe, Jane (Fed) <jane.doe@nist.gov>
Subject: Unpaid invoice #4806
How to Spot a Phish – What Can You Do?

• Be vigilant
• Consider your context. Does it make you vulnerable?
• Look for cues
  • Are there links, attachments, or requests for information?
  • Inspect carefully
• Use bookmarked links/favorites instead of clicking
• Use a search engine, don’t click on ads
• Consider calling the sender
• Clicking is the last resort!
How to Spot a Phish – What Can You Do?

• You are the last line of defense against a phishing attack
• Malware can make it past firewalls and filters
• Phone, postal mail, and in-person social engineering attempts can’t be detected with tools
• You are the Detective and Judge
• Every questionable email should be considered guilty until proven innocent
How to Spot a Phish – What Can You Do?

• What if you see a potential phish?

• Don’t:
  • Click on links
  • Download attachments
  • Provide any requested information

• Do:
  • Follow agency guidance for reporting suspicious emails
  • Contact sender through an alternative route
Summary

Multi-Pronged
Organizational phishing defense

Click rates
Click rates will not go to zero! (and stay there)

User context
Understand human element to contextualize click rates

No silver bullet
Awareness training is not the silver bullet in phishing defense
Additional Resources

- Jody Jacobs, jody.jacobs@nist.gov

- https://csrc.nist.gov/Projects/human-centered-cybersecurity
- https://csrc.nist.gov/Projects/human-centered-cybersecurity/research-areas/phishing
References


References


• Greene, Kristen & Steves, Michelle & Theofanos, Mary. (2018). **No Phishing beyond This Point.** Computer. 51. 86-89. https://doi.org/10.1109/MC.2018.2701632 (Accessed February 2023)