

SECURITY-MINDED

Practical security wisdom for daily life.



THE FACTS ABOUT PHISHING

Deceptive emails are a threat in the workplace and at home

What would you do if a suspicious stranger came up to you on the street and tried to lure you down a dark alley? You'd probably sense danger and either walk away quickly or call for help.

But what if the stranger approached you through email? You might feel it's safe to click on a link in the email or open an attached file — but it's a trap.

Every day, cyber criminals use malicious emails to try to scam individuals and organizations — a type of attack known as “phishing.” Interacting with a phishing email carries serious risks for you, your employer, even your family and friends. Fortunately, everyone can learn tactics for recognizing and avoiding these attacks.

What Is Phishing?

In a phishing attack, cyber criminals use deceptive emails to “fish for” information and lure people into falling for scams. These emails are carefully designed to trick you into revealing financial information, login credentials, or other sensitive data. Or, they may secretly install dangerous software (malware) that compromises your computer and the files on it.

Phishing emails typically pressure you to act quickly, without thinking. They

play upon strong emotions — such as curiosity, fear, or greed. These psychological manipulation tactics are sometimes known as “social engineering.”

Phishing emails also use a variety of technical tricks to steal information:

- **Malicious web links** – You're asked to click on a link that takes you to an imposter website or to a site infected with malware.
- **Malicious attachments** – You're urged to open an unexpected attachment that contains malware.
- **Fraudulent data-entry forms** – You're prompted to fill in sensitive information like user IDs, passwords, credit card data, and phone numbers.

Is Phishing Really My Problem?

Many companies have suffered serious data breaches that exposed everything from business secrets to the confidential data of millions of people. These data breaches often start by tricking one person with a phishing email, giving criminals a foot in the door.

Phishing can affect your personal life, too. Whether at home or at work, falling for a phishing email can have serious, long-term consequences.

Every day, cyber criminals use malicious emails to try to scam individuals and organizations — a type of attack known as “phishing.”

TIPS FOR FAMILY AND FRIENDS

Share what you've learned about phishing and ask family and friends about their cybersecurity knowledge or experiences.

- 1. Think before you click** – You shouldn't automatically trust any email message, especially if it sounds frightening or too good to be true. Familiar logos, senders' names, and personal information are often faked by scammers.
- 2. Be wary of unexpected requests for personal information** – Never send account numbers, PINs, or login credentials through email — even if the request sounds urgent.
- 3. Verify attachments before opening or downloading** – Even if an email seems to come from a company or person you trust, don't open an unexpected attachment. To make sure the file is legitimate, contact the company or individual directly through its website or use a known, verified phone number.

The Consequences of Falling for a Phish

At Work

- Loss of corporate funds
- Exposed personal information of customers and coworkers
- Outsiders accessing confidential communications, files, and systems
- Files becoming locked and inaccessible
- Damage to employer's reputation

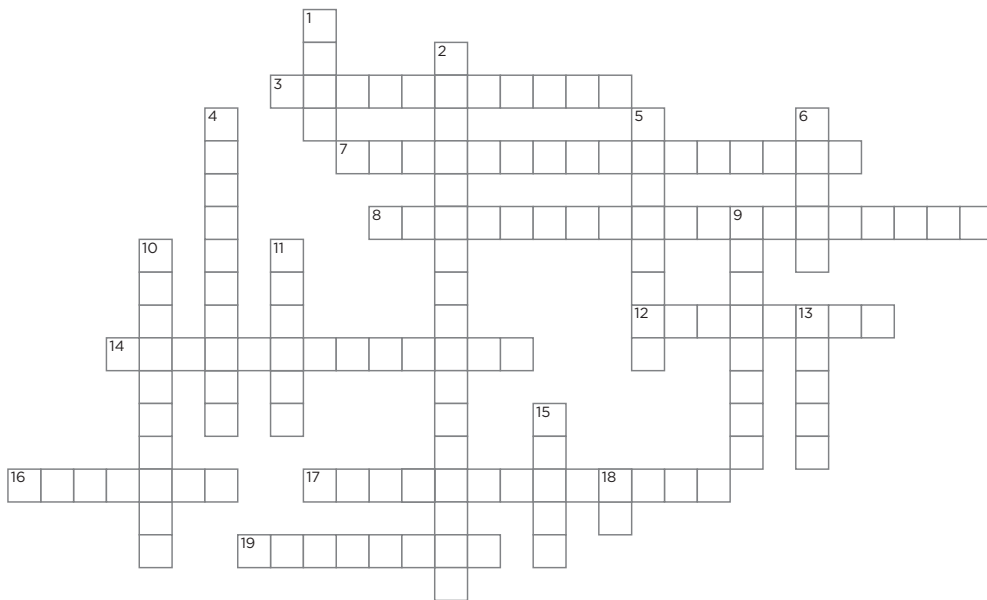
In Your Personal Life

- Money stolen from your bank account
- Fraudulent charges on credit cards
- Tax returns filed in your name
- Loans and mortgages opened in your name
- Lost access to photos, videos, and files
- Fake social media posts made in your accounts

What Can I Do?

- **Develop your anti-phishing skills.** Engaging with your organization's security awareness training program is a great way to practice identifying the warning signs of a phish.
- **Look for opportunities to learn more about phishing.** Additional articles in this series cover specific types of phishing and other security issues in more detail.
- **Find out how to report suspicious email.** Your organization's email platform may have a button that lets you quickly report potential phish. Or, you may need to forward the message to a specific IT inbox.

Activity Corner // Phishing 101 Crossword



Across

3. Sense danger?
7. Never send these via email
8. Looks real, but is infected with malware
12. Where to find additional information on the different types of (phishing)
14. Imposter website
16. Compromises computer and files
17. A stranger in a dark alley is much like a _____ in your inbox.
19. Who should learn how to recognize and avoid (phishing)?

Down

1. "Too good to be true"
2. Forgery, misdirection and lying are methods of
4. This can be damaged by falling for a (phish) at work
5. Falling for a (phish) in your ___ life could result in money stolen from your bank account
6. "Think Before You ___"
9. Security Awareness _____ can help you identify the warning signs of (phishing)
10. Exposes business secrets and confidential data
11. Before you open or download an attachment
13. Familiar ___ are often faked by scammers
15. Malicious email attack
18. Who do you report suspicious email to?

1 Trap, 2 Social Engineering, 3 Call for help, 4 Reputation, 5 Personal, 6 Click, 7 Login Credentials, 8 Malicious Attachment, 9 Training, 10 Data Breach, 11 Verify, 12 Articles, 13 Logos, 14 Malicious Link, 15 Phish, 16 Malware, 17 Cyber Criminal, 18 IT, 19 Everyone