

Phishing Schemes

Learn more about what these are, how they work, and how to spot them.

1. What Is a Phishing Scheme?

Phishing schemes are scams that do the following:

- Attempt to trick you into sharing or giving away valuable, personal information
- Attempt to trick you into performing a task or action (like clicking a link) that can install malware on your device

Hackers will often obtain things like email addresses in data breaches and then send out phishing scams to those emails in an attempt to fool or defraud you.

2. How Can I Spot a Phishing Scheme?

Phishing schemes can come in a variety of forms:

- Email
- SMS text
- Phone calls

They often use emotional appeals or different hooks in order to fool you. These might include:

- **Fear:** The scheme will tell you that you owe money or are in some sort of trouble to get you to panic and do what is being asked of you
- **Sympathy:** The scheme will tell you a sad story or gain your sympathy in order to convince you to do something
- **An opportunity or a prize:** The scheme will present a bogus opportunity to you (like a free trip) in order to get you excited and convince you to do something
- **Routine task or request:** The scheme will appear like it is a normal, common request from your workplace, for example

3. How Can I Detect Phishing Schemes?

Here are some tips for being cautious and avoiding phishing schemes:

- **Be careful with what you click or open**

Don't immediately click on or open things that seem odd or suspicious. If you weren't expecting to receive something, or if the request you get seems very urgent or alarming, slow down and check before you commit to any action

- **Check the sender of the email and any links**

Does the email address seem legitimate? With email phishing schemes, the name of the alleged sender might appear legitimate, but the email address will not match the sender's name. The link might also be a tinyurl or something suspicious. You can check by hovering over the link. Remember: don't click anything before checking first!

- **Consider the request**

Do you even have an account with this place? Think about what is being asked of you

- **Pay attention to the language of the request**

Phishing schemes might use odd greetings (such as "Hi dear" instead of your name) or strange phrasing. Typos, grammar errors, and other issues can also be a sign that this isn't from a legitimate organization. Also, pay attention to what you are being asked to do. Legitimate organizations will not ask you to share sensitive information on the phone, for example, or give away your password

- **Run a search**

Searching for what is being asked of you can be a great step to take! You can often find reports and articles on major, common phishing schemes and your search might help you confirm whether or not this is a scam

4. How Can I Avoid Phishing Schemes?

Make sure you are practicing good password hygiene and digital security!

- Keep your security settings up to date on your devices
- Use multi-factor authentication to add a layer of security to sites you use
- Backup your data

Good data security practices can help you keep your data and information secure and help you avoid falling prey to phishing schemes. But remember, phishing schemes are increasingly common and widespread. It's almost impossible to avoid them entirely, which is why recognizing them is important.

5. Reflect on Your Past Experiences

What sort of phishing schemes have you seen before? List some observations about what you have seen, encountered, or heard about here:

6. Test Your Knowledge and Skills

Test out your skills and learn to better spot phishing schemes with this activity:

- Test your skills with this Phishing Quiz from Google:
<https://phishingquiz.withgoogle.com/>
- After you've taken the quiz, work in small groups to review some common examples of phishing schemes on this site: <https://www.phishing.org/phishing-examples>
- See what trends you are noticing and what manipulation techniques are being used for these examples