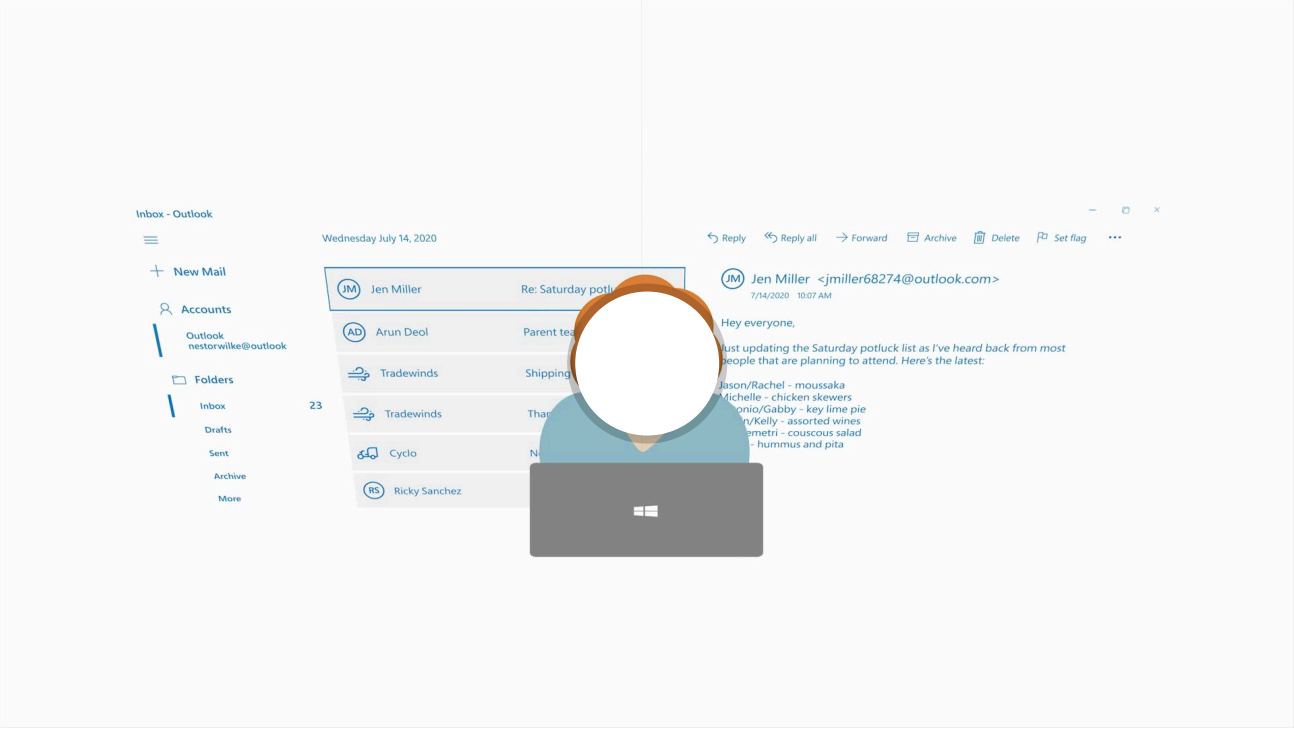
Protect yourself from phishing

Phishing (pronounced: fishing) is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as credit card numbers, bank information, or passwords -- on websites that pretend to be legitimate. Cybercriminals typically pretend to be reputable companies, friends, or acquaintances in a fake message, which contains a link to a phishing website.



Select the headings below for more information

Learn to spot a phishing message

Phishing is a popular form of cybercrime because of how effective it is. Cybercriminals have been successful using emails, text messages, and direct messages on social media or in video games, to get people to respond with their personal information. The best defense is awareness and knowing what to look for.

Here are some ways to recognize a phishing email:

- **Urgent call to action or threats** - Be suspicious of emails and Teams messages that claim you must click, call, or open an attachment *immediately*. Often, they'll claim you have to act now to claim a reward or avoid a penalty. *Creating a false sense of urgency* is a common trick of phishing attacks and scams. They do that so that you won't think about it too much or consult with a trusted advisor who may warn you.

  Tip: Whenever you see a message calling for immediate action take a moment, pause, and look carefully at the message. Are you sure it's real? Slow down and be safe.

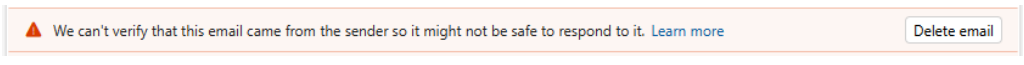
- **First time, infrequent senders, or senders marked [External]** - While it's not unusual to receive an email or Teams message from someone for the first time, especially if they are outside your organization, this can be a sign of phishing. Slow down and take extra care at these times. When you get an email or a Teams message from somebody you don't recognize, or that Outlook or Teams identifies as a new sender, take a moment to examine it *extra* carefully using some of the measures below.

- **Spelling and bad grammar** - Professional companies and organizations usually have an editorial and writing staff to make sure customers get high-quality, professional content. If an email message has obvious spelling or grammatical errors, it might be a scam. These errors are sometimes the result of awkward translation from a foreign language, and sometimes they're deliberate in an attempt to evade filters that try to block these attacks.

- **Generic greetings** - An organization that works with you should know your name and these days it's easy to personalize an email. If the email starts with a generic "Dear sir or madam" that's a warning sign that it might not really be your bank or shopping site.

- **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. Also be watchful for very subtle misspellings of the legitimate domain name. Like micros0ft.com where the second "o" has been replaced by a 0, or rnicrosoft.com, where the "m" has been replaced by an "r" and a "n". These are common tricks of scammers.

- **Outlook shows you a banner that says we could not verify the sender** - Outlook shows you this banner when something in the email headers is suspicious. Perhaps the email had failed authentication using commonly accepted internet standards. Perhaps the From field may have a value that deviates from industry standards in order to misrepresent the real sender and trick the email server. Whatever it is, you should remain cautious about the email content.



- **Suspicious links or unexpected attachments** - If you suspect that an email message, or a message in Teams is a scam, *don't open any links or attachments* that you see. Instead, hover your mouse over, but *don't click* the link. Look at the address that pops up when you hover over the link. Ask yourself if that address matches the link that was typed in the message. In the following example, resting the mouse over the link reveals the *real* web address in the box with the yellow background. The string of numbers looks *nothing like* the company's web address.

> **Tip:** On Android long-press the link to get a properties page that will reveal the true destination of the link. On iOS do what Apple calls a "Light, long-press".

Cybercriminals can also tempt you to visit fake websites with other methods, such as text messages or phone calls. If you're feeling threatened or being pressured, it may be time to hang up, find the phone number of the establishment and call back when your head is clear. Sophisticated cybercriminals set up call centers to automatically dial or text numbers for potential targets. These messages will often include prompts to get you to enter a PIN number or some other type of personal information.

For more information see How to spot a "fake order" scam.

> **Are you an administrator or IT pro?**
>
> If so, you should be aware that phishing attempts may be targeting your Teams users. Take action. Learn more about what to do about it here.
>
> If you have a Microsoft 365 subscription with Advanced Threat Protection you can enable ATP Anti-phishing to help protect your users. Learn more

If you get a phishing email or message in Teams

- Never click any links or attachments in suspicious emails or Teams messages. If you receive a suspicious message from an organization and worry the message could be legitimate, go to your web browser and open a new tab. Then go to the organization's website from your own saved favorite, or via a web search. Talk to them using official numbers or emails from their site. Call the organization using a phone number listed on the back of a *membership card*, printed on a *bill or statement*, or that you find on the *organization's official website*.

- If the suspicious message *appears* to come from a person you know, contact that person via *another means* like by text message or a phone call to confirm it.

- Report the message (see below).
- *Delete it.*

How to report a phishing scam

- **Microsoft 365 Outlook** - With the suspicious message selected, choose **Report message** from the ribbon, and then select **Phishing**. This is the fastest way to report it and remove the message from your Inbox, and it will help us improve our filters so that you see fewer of these messages in the future. For more information see Use the Report Message add-in.
- **Outlook.com** - Select the check box next to the suspicious message in your Outlook.com inbox. Select the arrow next to **Junk**, and then select **Phishing**.
- **Teams messages** - If you're in Microsoft Teams, hover over the malicious message withoutselecting it, and then select **More options > More actions > Report this message**. When asked to 'Report this message' choose the option *Security risk - Spam, phishing, malicious content is selected, and then select Report.* Click the **Report** button.

  If you are seeing signs of a scam, and are suspicious of a message, you, everyone else exposed to it, are better safe than sorry! Report it.

Note: If you're using an email client other than Outlook, start a new email to phish@office365.microsoft.com and include the phishing email as an attachment. Please don't forward the suspicious email; we need to receive it as an attachment so we can examine the headers on the message.

If you're on a suspicious website:

While you're on a suspicious site in Microsoft Edge, select the **Settings and More (...)** icon towards the top right corner of the window, then **Help and feedback** > **Report unsafe site.** Or click here.

Tip: ALT+F will open the **Settings and More** menu.

For more information see Securely browse the web in Microsoft Edge.

What to do if you think you've been successfully phished

If you're suspicious that you may have inadvertently fallen for a phishing attack there are a few things you should do.

1. 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.

2. 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.

3. Confirm that you have multifactor authentication (also known as two-step verification) turned on for every account you can. See What is: Multifactor authentication

4. 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.

5. If you've lost money, or been the victim of identity theft, don't hesitate, *report it to local law enforcement*. The details in step 1 will be very helpful to them.

See also

The keys to the kingdom - securing your devices and accounts

How malware can infect your computer

Need more help?

How can we help you?

Want more options?

Discover Community

Explore subscription benefits, browse training courses, learn how to secure your device, and more.

Microsoft 365 subscription benefits

Microsoft 365 training

Microsoft security

Accessibility center

Was this information helpful? Yes No

Payments

parents

Azure for students