



Internet safety

Phishing and malware attacks

ACCESSIBILITY

START >

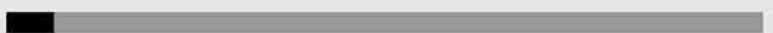


Cyber scams are growing

The internet has forever changed the way we communicate, share, work, learn, and play. And yet **the more dependent** on it we become, the **more we are exposed** to online threats.

With **over 1 billion phishing related attacks** in 2019 alone, these cyber scams are among the largest growing against consumers—and can result in very real consequences.

In this story, we'll discuss tips on protecting yourself from phishing and malware attacks and how the Microsoft ecosystem is working to help keep users safe.



An escalating challenge

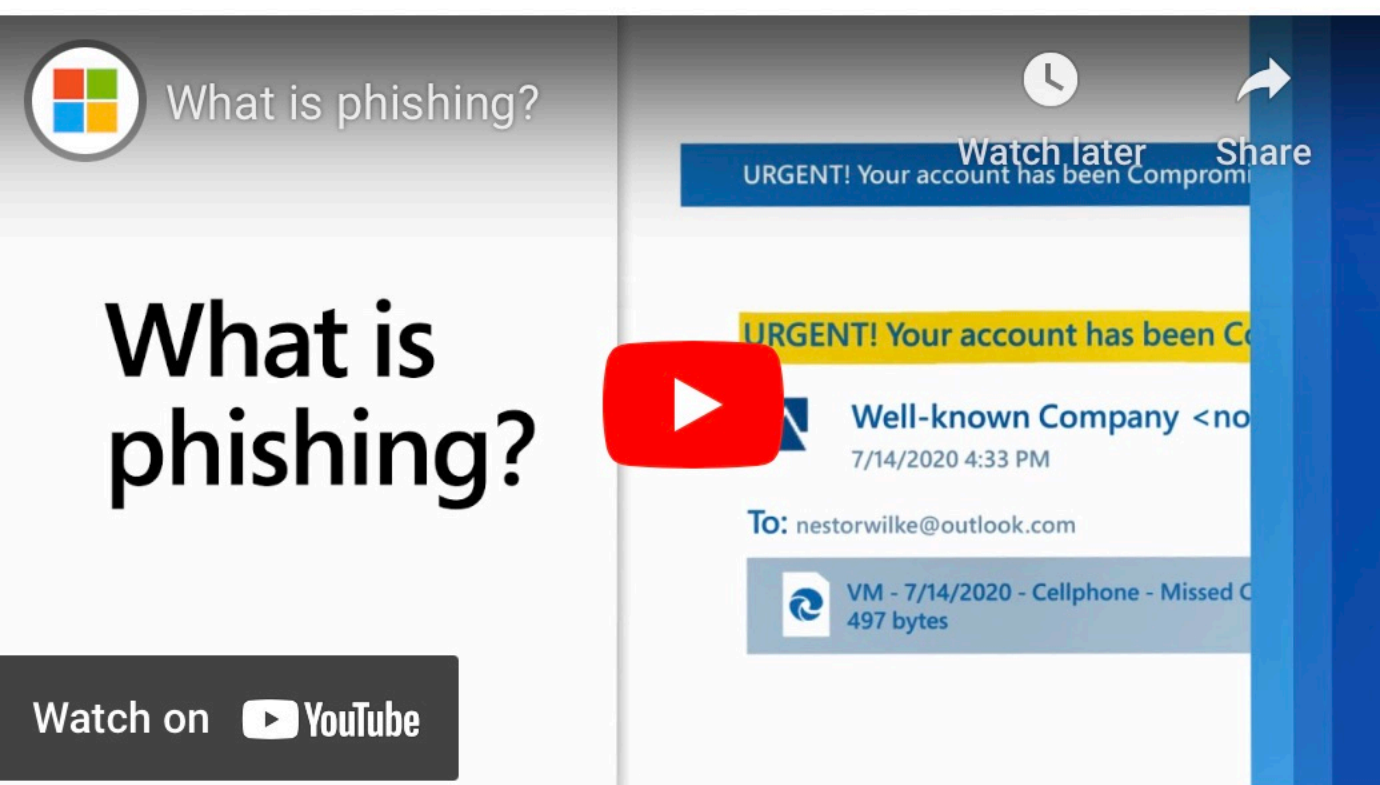


Cybercrime is an **ongoing and escalating challenge around the globe**. Now a large and diverse enterprise, **cybercrime** is often available for sale to commit a variety of attacks—such as fraud, theft, and spying. It could be financially motivated, or nation-state supported, or both.

Cybercriminals typically **pretend to be reputable companies**, friends, or acquaintances **in a fake message**, which contains a link to a phishing website.



Phishing scams



What is phishing?

Watch later Share

URGENT! Your account has been Compromised

URGENT! Your account has been Compromised

Well-known Company <no...>
7/14/2020 4:33 PM

To: nestorwilke@outlook.com

VM - 7/14/2020 - Cellphone - Missed Call - 497 bytes

Watch on YouTube

Phishing attacks **attempt 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.

A phishing email can be a massive campaign targeting millions of users, or a single, targeted email that was **many months in the making**.



Malware email attachments



Protect your devices and data fro...



Watch later



Share

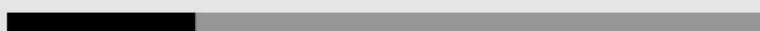
Protect
your devices
and data
from malware



Watch on  YouTube

Phishing and **malware often go hand-in-hand**. While phishing often involves sending spam emails to get you to click on links that take you to fake websites, malware authors use tricks to convince you to **download malicious files**.

They can **come in the form of an email with a file attached** that tells you it is a receipt for a delivery, a tax refund, an invoice for a ticket, or something similar. If you do open the file, you'll end up installing malware on your PC.



Malware downloads

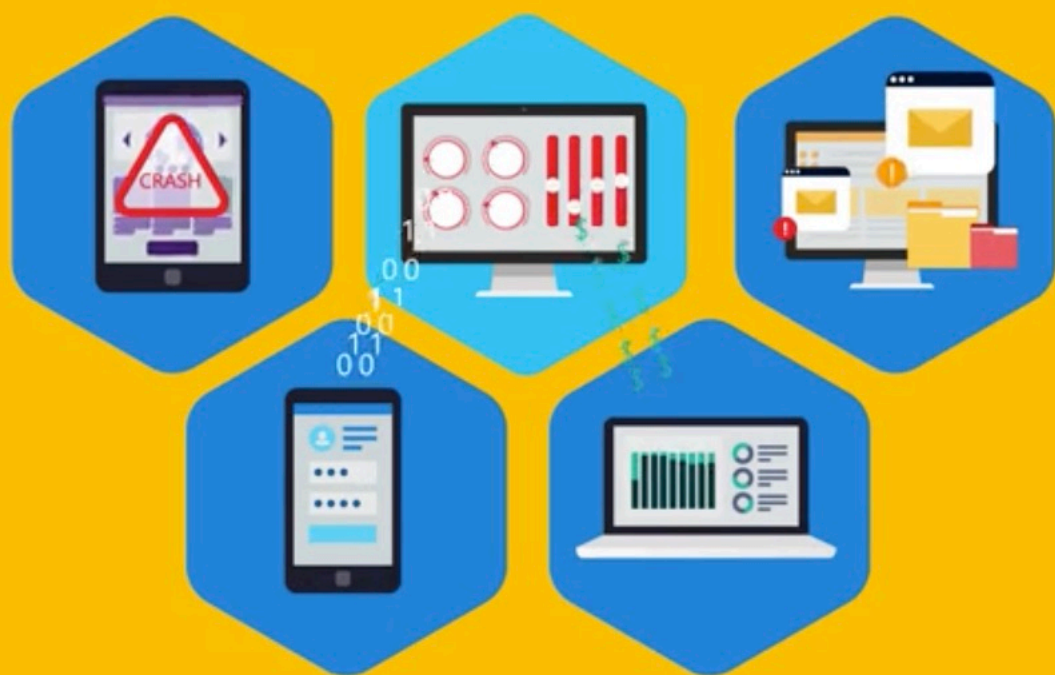


Some malware can be **installed at the same time as other programs that you download**. This includes software from third-party websites or files shared through peer-to-peer networks.

Some programs will also **install other software** that Microsoft detects as potentially unwanted. This can include **toolbars** or **programs that show you extra ads** as you browse the web.

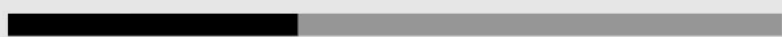


Botnets and Trojans



Botnets are networks of computers infected by malware that are **used to commit cybercrimes**. The cybercriminal or “bot master” uses special malware—called Trojans—that sometimes appear in an infected email attachment or in a link that you can be tricked into opening. They can cause your computer to send spam emails and run more slowly than usual.

While all of these threats may be concerning, there are ways to spot attacks. Let’s find out how.



Spotting malicious emails



Urgent call to action or threats

Be suspicious of emails 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.



Spotting malicious emails



First time or infrequent senders

While it's not unusual to receive an email from someone for the first time, this can be a sign of phishing. When you get an email from someone you don't recognize, or that Outlook identifies as a new sender, take a moment to examine it extra carefully before you proceed.



Spotting malicious emails



Spelling and bad grammar

Professional organizations usually have an editorial staff. If an email message has obvious spelling or grammatical errors, it might be a scam. It can be the result of incorrect translation from a foreign language or a deliberate attempt to evade filters that try to block these attacks.

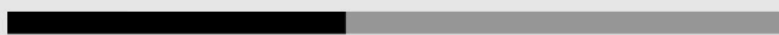


Spotting malicious emails



Generic greetings

If an email starts with a generic "Dear sir or madam" as opposed to addressing you by your name, that's a warning sign that it might not really be from your bank or shopping site.



Spotting malicious emails

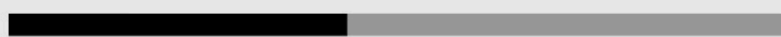
<https://www.woodgrovebank.com/loginscript/user2.jsp>



http://192.0.2.1/wood/index.htm

Suspicious links or unexpected attachments

If you suspect an email message is a scam, don't open any links or attachments that you see. Instead, **hover your mouse over**, but don't click, the link **to see if the address matches the link that was typed in the message.**

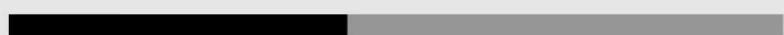


Spotting malicious emails



Mismatched email domains

If the email claims to be from a reputable company, but is being sent from another domain like `micros0ftsupport.rp`—it's likely a scam. Also be watchful for subtle misspellings of the legitimate domain name. Like `micros0ft.com` where the second "o" has been replaced by a 0.



Spotting malicious emails



Never click any links or attachments in suspicious emails.

If you receive a suspicious message, 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. You can also look up their number and call them.



Reducing your risk



With so many great things Microsoft is working on, there just isn't enough time to go over all the ways we're working to help keep our customers safe.

However, we've chosen some **helpful tips** we think will help you along your web (and email) browsing journeys.



Windows Security Center



The best protection from malware and unwanted software is an up-to-date, real-time security product, such as [Microsoft Defender Antivirus](#) **for Windows 10**—included at no cost on every Windows 10 device. It protects your device with **real-time virus and threat detection**, account, firewall and network protection, reputation-based protection, and more.



SCAN FOR THREATS >

TURN ON APP BLOCKING >



Running scans

If you suspect there's malware or a virus on your device, you should **immediately run a [quick scan](#)**. This is much faster than running a full scan on all your files and folders. ***To run a quick scan in Windows Security:***

1. Select **Start**  **> Settings**  **> Update & Security > Windows Security** and then **Virus & threat protection**.
2. Under **Current threats**, select **Quick scan** (or in previous versions of Windows 10, under **Threat history**, select **Scan now**).

To run a malware scan on a specific file:

When you're concerned about risks to a specific file or folder, you can right-click the file or folder in File Explorer, then select **Scan with Microsoft Defender**.

Learn more tips in the ExpertZone Story, [Microsoft Defender](#).



×

CLOSE



Turn on app blocking

Potentially unwanted applications (PUA) are a category of software that can cause your machine to run slowly, display unexpected ads, or at worst, install other software which may be more harmful or annoying.

To turn on potentially unwanted [app blocking](#) go to **Start**  **> Settings**  **> Update & Security > Windows Security > App & browser control > Reputation-based protection settings.**

You'll see a control that lets you turn potentially unwanted app blocking on, and select if you want to block apps, downloads, or both.

Potentially unwanted app blocking

Protect your device from low-reputation apps that might cause unexpected behaviors.

☒ On

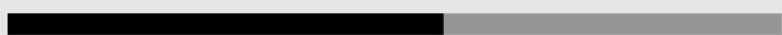
☒ Block apps

☒ Block downloads

[Protection history](#)



CLOSE



Outlook filtering & protection

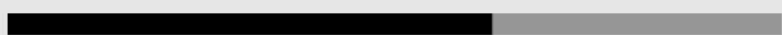


All Outlook.com users benefit from spam and malware filtering. Data encryption is provided for messages in your mailbox and after your email is sent.

Blocking is a great way to stop most unwanted senders. Select the spam email, then choose **Junk** from the drop down menu > **Block Sender**.

MICROSOFT 365 SUBSCRIBERS >

REPORTING SCAMS>



Extra protection

For Microsoft 365 Family and Microsoft 365 Personal subscribers **Outlook.com performs extra screening of the attachments and links in messages you receive.***

- **Attachments** to messages are scanned for viruses and malware using advanced detection techniques that provide a higher level of protection. If Outlook.com detects a dangerous file, it will be removed so you don't accidentally open it.
- **Automatic deactivation of unsafe links containing phishing scams, viruses, or malware.** If you click a link that is suspicious, you will be redirected to a warning page.
- **Ransomware detection and recovery** for your important files in OneDrive.

*Advanced security not available for @gmail.com and other accounts synced to an outlook.com account.



CLOSE



Reporting scams

If the suspicious message appears to come from a person you know, contact that person via some other means such as text message or phone call to confirm it. You can also report it:

In Microsoft 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**.

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**.



CLOSE



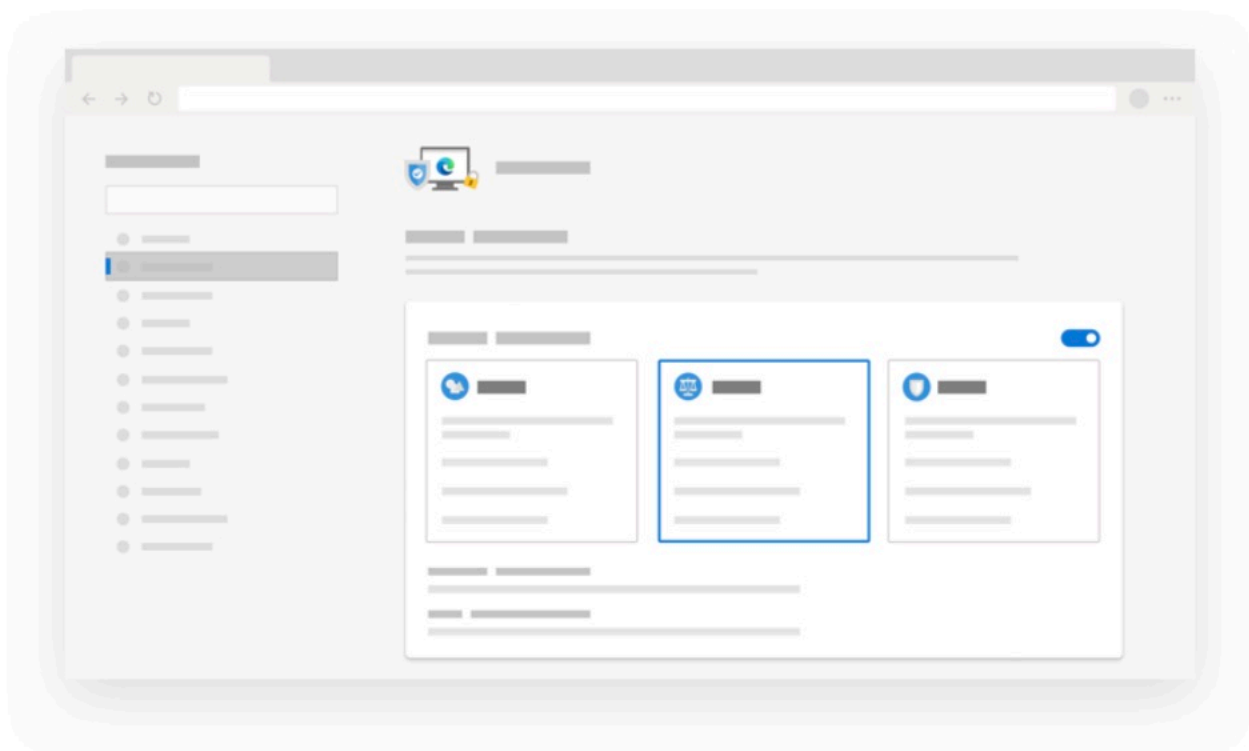
Microsoft Edge protection



Microsoft Edge is committed to helping our customers stay safe on the web to prevent unauthorized access of your browsing data. We put you in control—providing you with the information you need to make informed decisions. And we'll always honor your choices and collect only what is needed to make your experience better.



Microsoft Edge protection

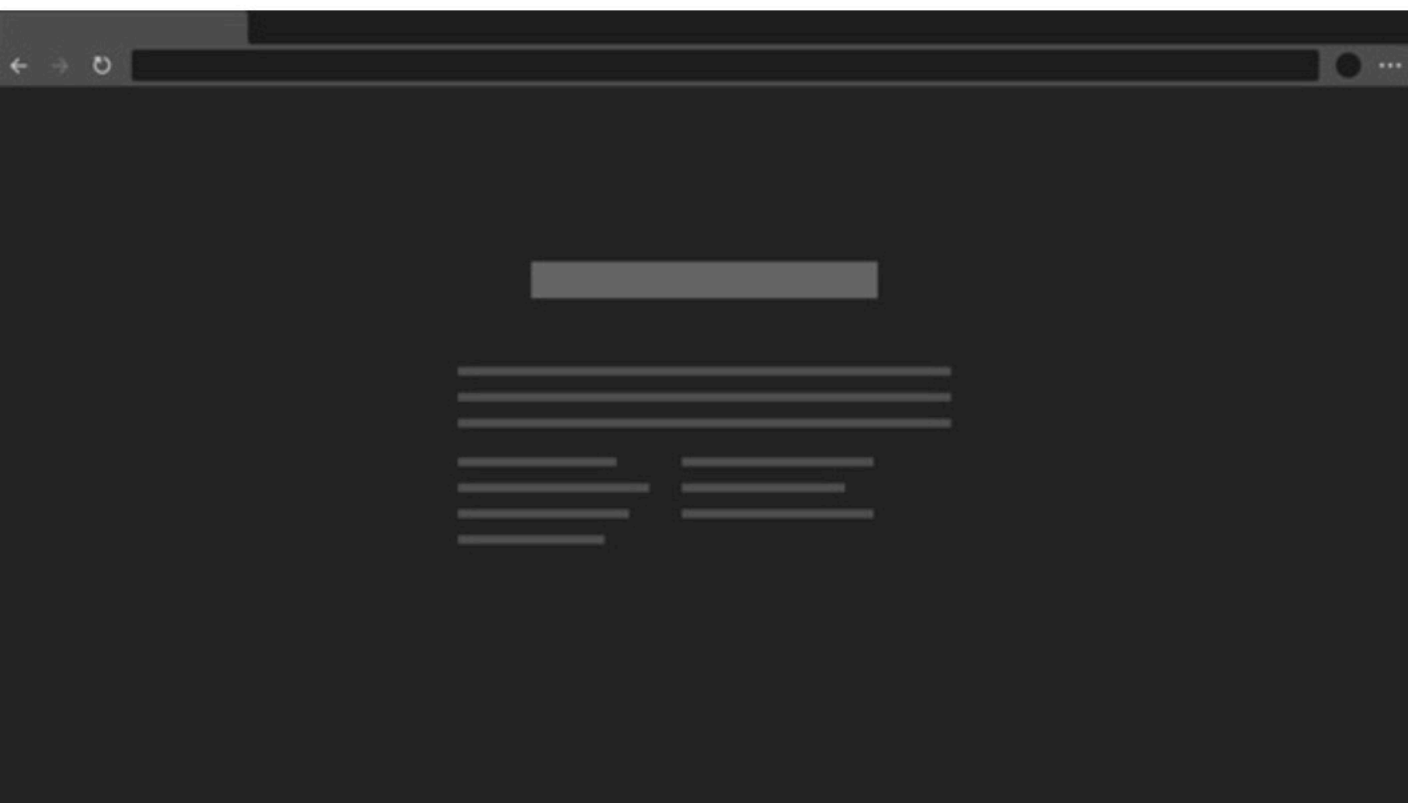


Control how you are tracked on the web

Website trackers collect data about how you interact with a site and other info about your browsing. Microsoft Edge is **designed to detect and block trackers**. We put you in control to decide what trackers to block. [Learn more](#) about tracking prevention.



Microsoft Edge protection



Keep your browsing and searching private

When you use [InPrivate tabs](#) or windows, your browsing and search data (like your history, temporary files, and cookies) **aren't saved** once you're done. We respect your decision and will **not tie your data** to your Microsoft account.

IF A WEBSITE IS SUSPICIOUS>



Suspicious websites

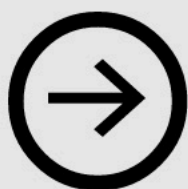
If you're on a website and get the feeling something just isn't right, you can easily report it.

- **Microsoft Edge.** While you're on a suspicious site, select the More(...) icon > Help and feedback > Report Unsafe site. Follow the instructions on the webpage that displays to report the website.
- **Internet Explorer.** While you're on a suspicious site, select the gear icon, point to Safety, and then select Report Unsafe Website. Follow the instructions on the webpage that displays to report the website.

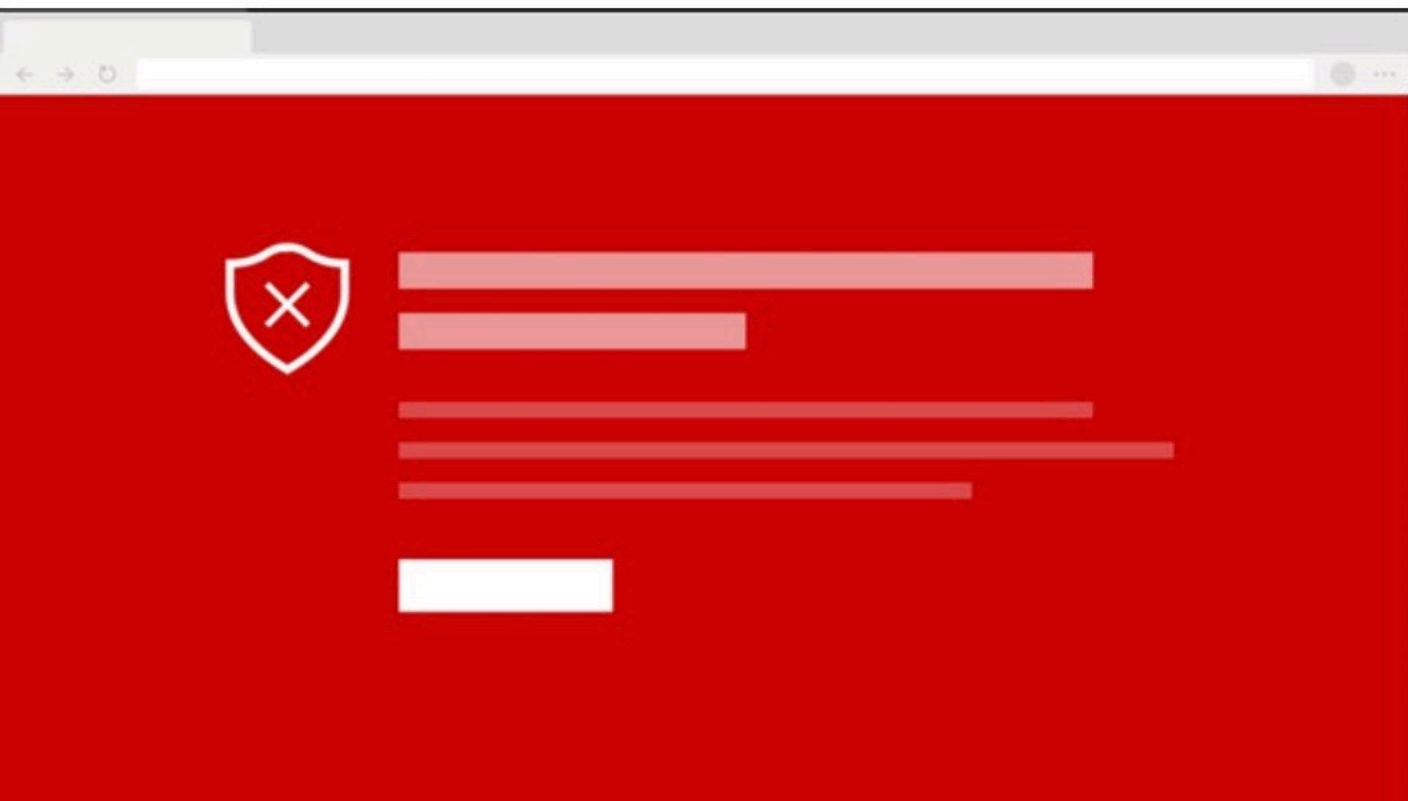
See [Securely browse the web in Microsoft Edge](#) for more ways to help you determine if a site is safe for browsing.

×

CLOSE



Microsoft Edge protection



Stay safe from malicious sites and downloads

Microsoft Edge comes with **Microsoft Defender SmartScreen built-in** and is turned on by default in Microsoft Edge—**protecting you against phishing or malware websites**, and from downloading potentially malicious files.

HOW TO DETERMINE IF A SITE IS SAFE>



Is the website secure?

As you browse, the following icons tell you if the website you are visiting is secure.



Connection secure/ valid certificate

The information sent to and from the site is secure and can't be intercepted by an attacker.



Not fully Secure (no valid certificate)

Information is not secure and can be intercepted by an attacker or seen by others. There's a risk to your personal data on this site.



Outdated security configuration (not valid, expired, self-signed) Something is severely wrong with the security of the site. The information sent to and from it is not secure and can be intercepted.



Suspicious or dangerous website (phishing or malware)

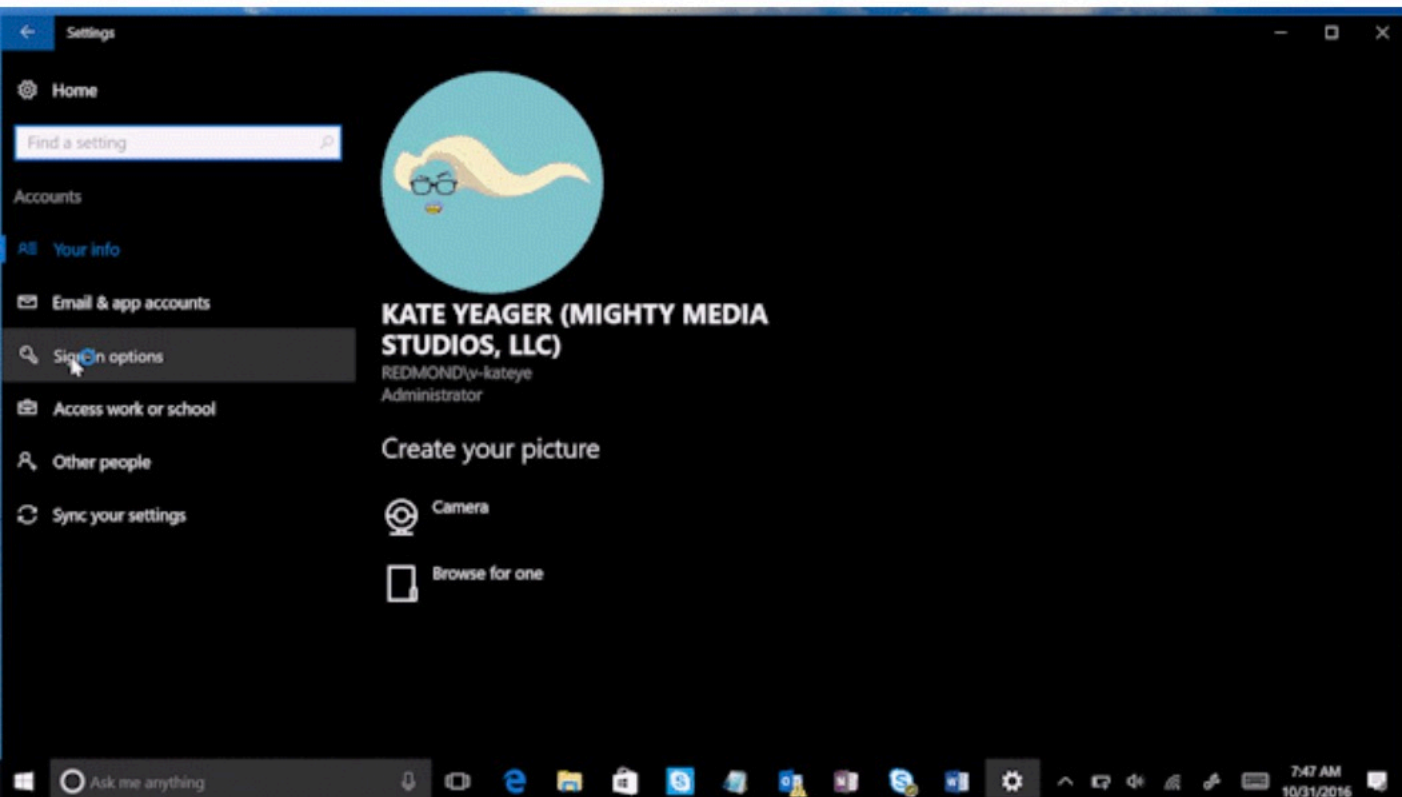
This website has been flagged by Microsoft Defender SmartScreen and you should avoid it. Using this site will put your privacy and security at risk. It may be trying to trick you into installing something dangerous. [Learn more.](#)



CLOSE



Windows Hello



Phishing attacks are often targeted at obtaining your passwords and identifying information.

Windows Hello helps protect you by providing a more personal and secure way to sign in to your devices, apps, and favorite websites. Depending on your organization and device, options include multi-factor authentication and biometrics—such as your face, fingerprint, or PIN.*

*Windows Hello requires specialized hardware including a Windows Hello capable device, fingerprint reader, illuminated IR sensor or other biometric sensors and capable devices.

SEE IF YOU HAVE WINDOWS HELLO>



Do you have Windows Hello?

To check to see if your device works with Windows Hello, go to:

Start  **> Settings**  **> Accounts**  **> Sign-in options.**

Under **Manage how you sign in to your device**, select a Windows Hello item to add, change, or remove.

Depending on the device, options include:
Windows Hello Face, Windows Hello Fingerprint, Windows Hello PIN.

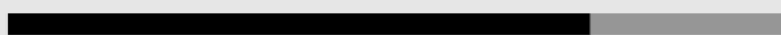
To add Windows Hello as a sign in method for your Microsoft account:

Go to the [Microsoft account page](#) **sign in > Security > More security options > Add a new way to sign in for verify > Use your PC.**

*For more helpful tips, check out the **ExpertZone Story**, [Windows Hello](#).*

×

CLOSE



OneDrive protection



If you do happen to download a malicious file to OneDrive, you'll [get a notification](#) on your device and receive an email from Microsoft 365.

You'll be guided through the process of restoring your files—starting with a [confirmation](#) that your files are infected. You'll then be able to [clean all your devices](#) and [restore your OneDrive](#). If you're not a subscriber, your first notification and recovery is free.



If you've been phished

- Write down as many details of the attack as you can recall. Try to **note any information** such as usernames, account numbers, or passwords you may have shared.
- Immediately **change the passwords** on those affected accounts, and anywhere else that you might use the same password.
[Create unique passwords](#) for each account.
- **Turn on [multifactor authentication](#)** (also known as two-step verification) for every account you can.
- If this attack affects your work or school accounts, you should **notify your IT support** of the possible attack. If you shared information about your credit cards or bank accounts you may want to contact those companies to **alert them to possible fraud**.
- If you've lost money, or been the victim of identity theft, **report it to local law enforcement**. The details you've provided will be helpful in their investigation.



How you can help



You can assist Microsoft by **submitting unknown or suspicious software for analysis**. This will help ensure that unknown or suspicious software is scanned by our system.

[Submit a file for malware analysis](#)

You can also **report tech support scams** whether they claim to be from Microsoft or from another tech company:

[Report Microsoft technical support scams](#)





Internet safety is a top priority

While cybercriminals may think they've got the inside track on getting you to part with your information (and money)—Microsoft is actively creating solutions to **reduce your risk across our entire ecosystem.**

Let your customers know we understand the role we play in providing a safer internet experience for our customers, and that we care about their concerns.

And remember to keep checking ExpertZone for more helpful tips on all your favorite Microsoft apps and tools!



Select 'X' to close.