How to turn on Enhanced Phishing Protection on Windows 11 to display warnings when entering passwords into Notepad and websites

Windows 11 22H2 has just been released and with it comes a new security feature called Enhanced Phishing Protection with the ability to warn users when they enter Windows passwords into unsafe applications or on websites.

Hackers often steal these passwords through phishing attacks or by users saving passwords in insecure applications, such as word processors, text editors, and spreadsheets. .

In some cases, just by entering the password into the fraudulent login form and not clicking submit, your password has been stolen by hackers.

To prevent this, Microsoft has introduced a new feature called Enhanced Phishing Protection on Windows 11 22H2 with the ability to warn users when they enter Windows passwords into unsafe applications or on websites.

"SmartScreen identifies and protects against password entering on phishing websites or apps connected to phishing websites, password reuse across any app or website, and passwords being imported into Notepad, Wordpad or Microsoft 365 apps ," explains Microsoft Security Product Manager Sinclaire Hamilton.

"IT admins can set up which situations require alerts to be sent to end users via CPS/MDM or Group Policy" .

At the moment, this new feature is currently only available on Windows 11 22H2 and it is not enabled by default. It also requires you to sign in to Windows with your Windows password instead of using Windows Hello.

Therefore, when you use a PIN to sign in to Windows, this feature will not work.

When enabled, Microsoft will detect when you enter your Windows password and then issue a warning prompting you to remove the password from an insecure file or, when entered on a website, to change your Windows password. .

How to turn on Enhanced Phishing Protection

Although Windows 11 22H2 has anti-phishing protection enabled by default, your password protection option is disabled.

To enable this option, you need to go to Start > Settings > Privacy & security > Windows Security > App & browser control > Reputation-based protection settings.

In the Phishing protection section, you will see two new options: "Warn me about password reuse" and "Warn me about unsafe password storage".

When enabled, the "Warn me about password reuse" option will display a warning when you enter your Windows password on a website whether it is a phishing website or a legitimate website.

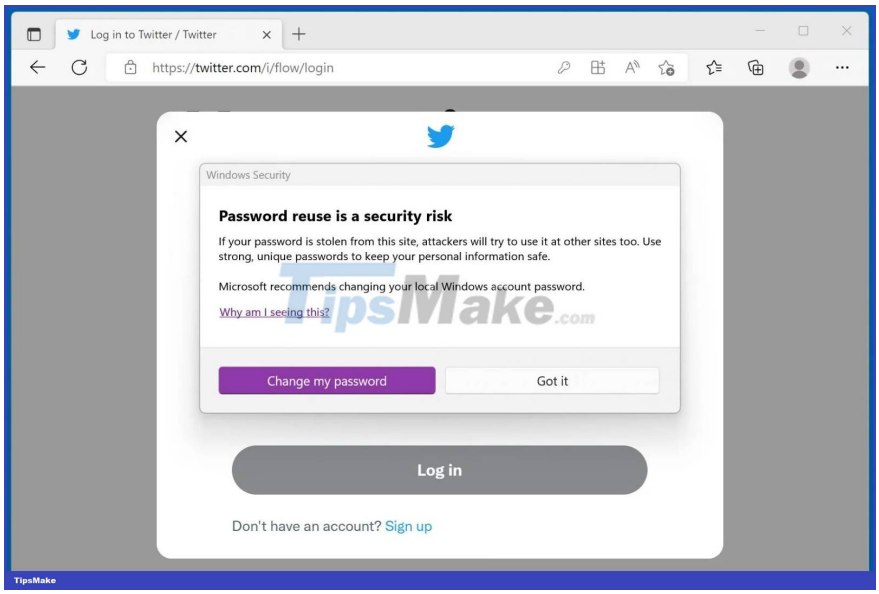
Meanwhile, the "Warn me about unsafe password storage" option will display a warning when you enter passwords into applications like Notepad, Wordpad, and Microsoft Office then press Enter.

To protect your password, check both of these options to enable them. As you enable each option, Windows 11 displays a UAC prompt for you to confirm the settings.

In Bleeping Computer's test below, Windows 11 displays a warning when entering a password into Notepad and pressing Enter. Accompanying the warning is advice that users should remove the password from the file. Other applications that also display warnings include WordPad and Microsoft Word 2019.

However, it does not display a warning when entering passwords in Excel 2019, OneNote and Notepad 2. This needs to be reviewed and corrected because Excel is often used if it is necessary to create a list of passwords.

Another thing to note is that Windows 11 only displays warnings when using Google Chrome and Microsoft Edge. Similar test on Mozilla Firefox, the warning does not appear.



Overall, this is a great security feature for Windows users, and you should use it to protect yourself from phishing attacks and avoid saving your passwords in insecure applications.

However, there's still a lot of room for improvement, and Microsoft needs to expand this security feature to support more browsers and apps.

You finished reading the article "**How to turn on Enhanced Phishing Protection on Windows 11 to display warnings when entering passwords into Notepad and websites**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.