Microsoft

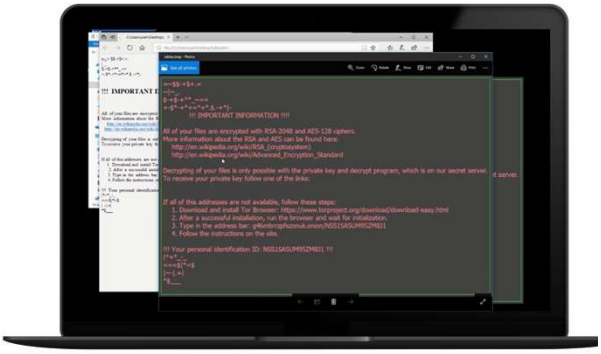
Cybersecurity Simplified: Ransomware

Ransomware is malicious software that blocks access to a computer system or files unless a sum of money is paid.

Ransomware twists the power of encryption against you. Encryption should protect your data and files, but ransomware uses it to take files hostage. This means being locked out of your documents, spreadsheets, photos and videos, and other important files. Plus, an infected PC can spread the ransomware to other computers on your network.

Example scenario

Your employee receives an email from a friend. It includes a link to a video that shows how to make heart shapes out of boiled eggs using chopsticks. Intrigued, your employee follows the link and is asked to click Run.



Later that day, everything on their screen starts changing colors, and a window appears informing them that all the files on the computer have been hijacked and encrypted.

They won't be able to access anything, unless they pay a ransom. If they choose to not pay, they may never get access to the files again.

Three ways Microsoft 365 Business protects your company against ransomware

Microsoft 365 Business helps protect against malware and other malicious content **sent via email**. All messages with unknown attachments are routed to a special "sandbox" environment, and if suspicious activity is detected, the email is not released to the mailbox. Additionally, the Safe Links feature helps to protect against malicious links in emails by checking the hyperlink each time it is clicked, and the destination is blocked if it is deemed to be malicious.

Microsoft 365 Business uses Windows Defender Exploit Guard to help **protect devices**. Exploit Guard prevents unauthorized access to common folders such as Desktop or Documents. This means that unauthorized apps, scripts, and executable files won't be allowed access, so any ransomware that attempts to hijack and encrypt your files in these locations will be blocked. The user is informed that the file has been blocked via a small notification window.

Microsoft 365 Business also helps to **recover files** in the event of a successful ransomware attack. Files stored in OneDrive for Business (the cloud storage service included in Microsoft 365 Business) are automatically versioned, which allows you to recover versions of items that pre-date their encryption by the ransomware, with just a few clicks.

Microsoft's approach and commitment to enhancing security

Ransomware continues to evolve and impact many types of devices in different environments. Microsoft continues to invest in innovative solutions to protect your business against ransomware and other threats.

- Microsoft's security solutions are built into our products, so there is nothing additional to deploy or manage
- Microsoft spends over $1 billion annually on security alone.
- Microsoft's analytics and cloud-based capabilities use advanced data science approaches to make sense of the world's largest set of threat-related optics and turns them into actionable intelligence that our defenses can react to.
- Windows Defender pre- and post-breach defenses are built deep in the OS making them resistant to tampering by malware and hackers

Get started:

Learn more about Microsoft 365 Business at www.microsoft.com/microsoft365/business