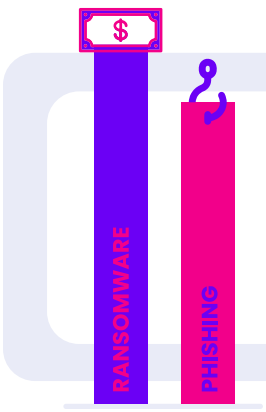
Ransomware: 4 Reasons Email is the #1 Delivery Method

Globally, ransomware caused $20 billion in damages in 2020.[1] While there are numerous ways to launch a ransomware attack, many methods are complex, time-consuming, and expensive to execute. The fastest and cheapest way to deliver ransomware is with the most used communication tool in the world: email.

1. Phishing emails are easy to create

It doesn't take a high level of skill to create a phishing email. To create the illusion of legitimacy, hackers mimic a brand's look and feel by using brand images and logos from the target brand's website or Google images.



67%
of ransomware infections were delivered via phishing/spam.[2]

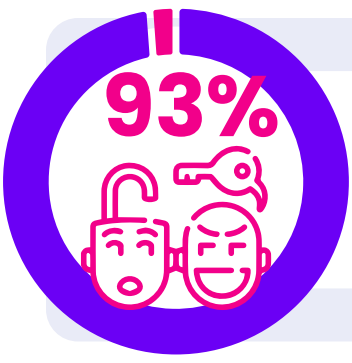
2. Ransomware kits are cheap

For around $66.00 hackers can purchase a ransomware kit online, and purchase a monthly subscription for double the price. This reduces the level of effort for the hacker and makes the attack that much easier to deploy via email.[3]

$66
typical cost of a ransomware kit.

3. Social engineering helps hackers craft the perfect email

Social engineering manipulates victims into divulging sensitive information or taking a desired action. Hackers can easily find information about employees online, especially on social media platforms, to craft the perfect ransomware email.



93%
of successful breaches were caused by social engineering [4]

4. Email attachments and shared files can deliver the payload

Links hidden in attachments download malware at the time of click. In other cases, the ransomware download begins automatically when the attachment is opened, often via macros in Word docs and PDFs or malicious scripts in .zip files.

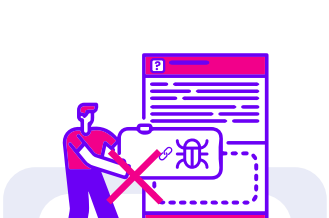
40%
of malware is deployed via email attachments.[5]

Protect your business from ransomware

When ransomware arrives on your business's doorstep, it will be in an email.
Follow the below tips to protect your business from attack:

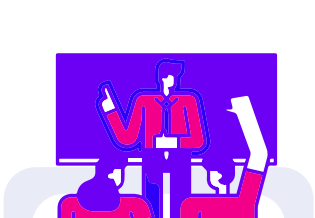
Think before you click:

Scrutinize email addresses for unusual characters and extensions, and hover over links to see the real destination of the URL.



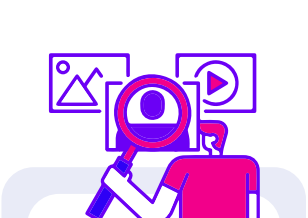
Never open attachments from unknown senders:

The think before you click rule also applies to attachments. If the sender is suspicious, do not open the attachment.



Train your users:

Provide ongoing user awareness training, as well as post-incident training to reinforce cybersecurity best practices.



Add an additional layer of email security:

An additional layer of email security can provide reinforcements. Choose a solution that explores URLs, attachments, shared files, images, and webpages.

[1] Barrons. https://www.barrons.com/articles/2020-was-a-bad-year-for-ransomware-2021-will-be-worse-51610124513

[2] Statista. https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/

[3] AtlasVPN. https://atlasvpn.com/blog/most-damaging-cybercrime-services-cost-less-than-500-on-the-dark-web

[4] Verizon. https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

[5] Ibid.

To learn how Vade for M365 can protect your business from ransomware, contact Vade.

About Vade :

- 1 billion mailboxes protected
- 100 billion messages analyzed per day
- 1,400 partners
- 95 percent renewal rate
- 17 active AI patents

Learn more :

www.ictnetworksystems.ca/vadesecure

Contact :

Sales

ictnet@ictnetworksystems.ca