Ransomware Awareness Email Template

Ever since the global WannaCry incident in May 2017, ransomware has been the most talked-about security topic in the country. Ransomware is growing quickly in popularity because businesses continue to pay to free up their data. And as long as hackers keep getting rewarded for their efforts, ransomware will continue to be a go-to strategy. Stopping it isn't easy - but it starts by knowing what to look for. The email below can help educate your employees on the warning signs of a ransomware attack.

Dear team,

In an effort further enhance our company's cyber defences, we want to highlight a common cyber-attack that everyone should be aware of – ransomware.

Ransomware is increasingly being used by hackers to extort money from companies. Ransomware is a type of malicious software that takes over your computer and prevents you from accessing files until you pay a ransom.

Although we maintain controls to help protect our networks and computers from this type of attack, with the quickly changing attack scenarios we rely on you to be our first line of defence. Here are some simple things you can do to help [COMPANY NAME] avoid a ransomware/malware attack:

Think Before You Click

The most common way ransomware enters corporate networks is through email. Often, scammers will include malicious links or attachments in emails that look harmless. To avoid this trap, please observe the following email best practices:

- *Do not click on links or attachments from senders that you do not recognize. Be especially wary of .zip or other compressed or executable file types.*
- *Do not provide sensitive personal information (like usernames and passwords) over email.*
- *Watch for email senders that use suspicious or misleading domain names.*
- *If you can't tell if an email is legitimate or not, please [INSERT COMPANY PROTOCOL].*
- *Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.*

If Something Seems Wrong, Notify IT

If your computer is infected with ransomware, you will typically be locked out of all programs and a "ransom screen" will appear. In the unfortunate event that you click a link or attachment that you suspect is malware or ransomware, please notify IT immediately.

To contact IT, please [INSERT COMPANY PROTOCOL].

Thanks again for helping to keep our network, and our people, safe from these cyber threats. Please let us know if you have any questions. Regards, [NAME]