Identifying and Responding to Ransomware Attacks

Ransomware is malicious software that infects a device and either prevents it from working as intended or restricts access to certain files until the target pays a ransom. Typically, the cybercriminals behind ransomware demand payment in cryptocurrency, such as bitcoin, which allows them to collect funds outside the traditional banking system. Businesses of all sizes have become targets of ransomware, as it can infect not only personal devices but also entire networks and servers.

Employees are often the initial targets in ransomware attacks due to their access to valuable corporate systems, funds and data. These attacks often start with phishing scams, in which cybercriminals leverage deceptive emails or other forms of communication to manipulate employees into visiting unsafe websites, clicking on harmful attachments or downloading dangerous programs that ultimately launch malicious software.

When these incidents occur, they can lead to prolonged operational disruptions and serious financial challenges for your employer. In fact, these attacks are among the costliest cybercrimes, resulting in billions of dollars in losses each year. As such, it's crucial that you play your part in preventing these attacks. This article explains what ransomware does to a device, outlines potential warning signs and offers related mitigation strategies.

What Ransomware Does to a Device

There are two main types of ransomware that can hold devices (and any systems and data stored on them) hostage. This includes:

- **Lock-screen ransomware**—This software works by displaying a window on the device's lock screen that attempts to prevent access to it. The message on the lock screen may even claim to come from the federal government, accuse the target of violating a law and demand a fine.
- **Encryption ransomware**—This software works by keeping the device available but encrypting certain types of files, thus making them unreadable. The files most commonly targeted are those containing sensitive information, which cybercriminals assume are of the greatest value. When people try to access the files, they see a pop-up screen that instructs them to buy a private decryption key to unlock the scrambled files.

Some operating systems provide instructions for responding to lock-screen ransomware, although results aren't guaranteed. In contrast, encryption ransomware has no quick fix without an encryption key, which only the cybercriminals typically have access to.

Warning Signs of an Attack

In the lead-up to a ransomware attack, you may notice the following warning signs on your device:

- Sluggish performance (e.g., applications taking longer to open or closing unexpectedly, websites loading slower than normal or simple tasks freezing)

ONEDIGITAL

Provided by OneDigital – Carolinas

- Files suddenly being renamed, using unfamiliar extensions or restricting access
- Unusual network activity, especially within shared drives and cloud storage

While these issues can occur, they may not be obvious. In some cases, you might not detect any warning signs of a ransomware attack, with the first and only indicator being a locked screen or ransom note.

Mitigation Strategies

The best way to mitigate a ransomware attack is to prevent it from occurring in the first place. This primarily entails keeping all security software on your device up to date, creating complex and unique passwords across your workplace accounts and enabling any additional company safeguards, such as a virtual private network, data encryption tools, firewalls, patch management systems, antivirus programs and multifactor authentication services. Ask your employer for more information on these resources.

Furthermore, since many ransomware attacks stem from phishing scams, it's best to be prepared to identify key indicators of these scams (e.g., unknown or copycat senders, generic or threatening language, unsolicited links or attachments and unusual or sensitive requests) and act accordingly. Never respond to these messages or answer any prompts without first verifying them through an alternative channel.

Even with these precautions in place, ransomware attacks may still occur. If you notice any warning signs of an impending attack, experience a locked screen or receive a ransom note, take these steps to help minimize the damage:

- **Don't interact.** Never interact with a ransom note or comply with other demands from a cybercriminal. Regardless of the circumstance, experts advise against paying the ransom, as there's no guarantee the cybercriminal will restore your device after payment. By paying the ransom, you could also be encouraging future cybercrimes against your employer. In addition, don't panic or take matters into your own hands by trying to recover any affected systems or data yourself, as this could cause more harm than good.
- **Report it.** Whether it's suspected or genuine, inform the IT team of the incident immediately. From there, the team will determine appropriate next steps. In some cases, this may involve internal remediation efforts. For more severe incidents, this may entail an in-depth investigation with the Cybersecurity and Infrastructure Security Agency (CISA), the FBI and local authorities.
- **Document any evidence.** Depending on the nature of the attack, you may be asked to share any relevant details you can recall about the incident, such as initial warning signs and ransom note phrasing. With this in mind, be sure to take notes regarding what you noticed and when. This could help support the investigation process and promote a faster recovery.

For More Information

Ransomware poses a serious threat to both your device and your employer's broader systems and data. By staying alert to warning signs, practicing strong cyber hygiene and knowing how to respond if an attack occurs, you can help minimize the associated damage and disruptions.

Cybersecurity can be challenging, but you don't have to navigate this topic alone. Reach out to your employer for more information on cybersecurity best practices.