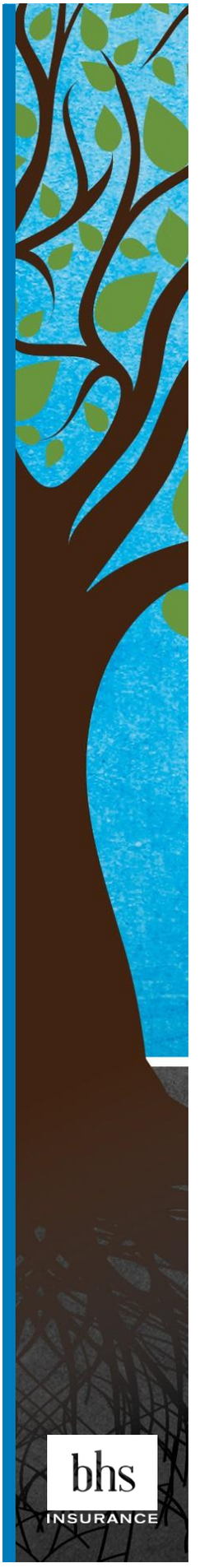
The Rising Concern over Ransomware and Phishing Email

By BHS Insurance

December 2019



Ransomware is a growing concern for non-profits of all sizes but can be prevented with strategic risk management practices to counter these attacks and protect critical infrastructure and data. As they say "it is not a matter of if, but when" you will be threatened, consequently it is important to be prepared.

What is Ransomware?

Ransomware is a malicious software created to deny access to computer and phone systems until a ransom is paid. Ransomware can be spread in a variety of ways: a phishing email that appears as a legitimate invoice, image or link, a visit to an infected website or an ad containing malware that has been injected into a legitimate webpage. When an unsuspecting victim opens an email or inadvertently falls into an online trap containing ransomware, the virus is silently installed on the victim's computer.

Ransomware manifests in different ways. Lock screen ransomware displays a window that prevents access to any part of the computer until a ransom is paid, while file-encrypting ransomware keeps the computer available but scrambles certain files and databases, then displays a pop-up screen with instructions on how to buy a private decryption key that will unlock the scrambled files.

Human Error

Human Error is the number one reason that ransomware is allowed to infiltrate your computer system. Some statistics state that phishing emails are clicked on by employees 8 to 20 percent of the time, depending on content. To make matters worse, phishing scams grew nearly 41 percent in 2018.

Of the businesses affected by ransomware 45 percent ultimately paid the hackers, but only 26 percent had their files unlocked. The most recent industry indications show that full restoration can take up to thirty days and the average cost of an attack – including the ransom fee and associated business losses – totaled more than $900,000. It's worth noting that attacks against small and medium sized businesses are on the rise and public gardens are no exception.

Protection from an Attack

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) recommends the following steps to protect your institution from a ransomware attack:
https://www.cisa.gov/blog/2019/08/21/cisa-insights-ransomware-outbreak

- Update software and operating systems with the latest patches. Outdated applications and operating systems are the target of most attacks.
- Never click on links or open attachments in unsolicited emails. There are four primary attributes of a phishing email:

1. There is new or changed information in the content of the email.
2. A sense of urgency.
3. Leadership staff are out of the office.
4. Ramification if the transaction is not processed promptly.

Spend time training your staff on how to recognize phishing emails and reiterate the importance to "question and confirm" in person before processing any requests.

- Backup data on a regular basis. Keep it on a separate device/cloud and store it offline. Test your back up frequently and know the timeline it will take to be back up and running.
- Restrict users' permissions to install and run software applications, and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Be sure to enable strong passwords along with multi-factor authentication.
- Follow the NIST 5 Reasonable Security Measures; Identify Protect, Detect, Respond and Recover.
  https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc
- Align yourself with trusted experts to help you audit your systems and test them.

Cyber Insurance Protection

Consider purchasing Cyber Insurance including Social Engineering Coverage to assist with breach response services and funding out of pocket costs related to forensic investigation, legal costs, public relations, revenue interruption and privacy breach notification. The policies available often provide access to services to assist in staff training and key cyber risk management tools.

Train employees in cyber security as it will not only help them while working but also in their personal cyber protection at home. Keep training fun and encourage employees to report any concern or suspect email so they are comfortable to ask before responding. Maintaining a culture of readiness and response will help protect your public garden from these continuing threats.

For more information, please contact a garden team member at BHS Insurance at (800) 350-7676.