CYBERSECURITY – TIPS TO STRENGTHEN YOUR RESISTANCE TO BAD ACTORS

Congregations and councils are soft targets for hackers. They typically do not have Information Technology (IT) departments and cannot afford IT consultants or sophisticated programs to protect their systems. To protect against cyber-intrusions and threats such as ransomware, councils and congregations should consider implementing basic cybersecurity strategies and direct training for employees. Such steps include:

1. Setting up a regular schedule to **update software** on all devices used by employees. Preferably, turn on the automatic updates function on all devices.
2. Make sure the software updates include **security patches** recommended by your software vendors.
3. Make sure devices in the office are secured, meaning, they are locked in an office when an employee leaves that office, or they are connected to a work desk by cable so they cannot be removed. **Physical security** of devices is as important as cyber security.
4. Use Apple's Find my iPhone or the Android Device Manager tools to help prevent loss or theft of employee devices.
5. Encourage employees who take home their devices (phones, laptops, etc.) not to leave them unattended in public places, such as coffee shops. They are responsible for their devices and their security. Again, physical security is as important as cyber security.
6. Ensure that all devices come with a superior quality **firewall**. This is usually standard on devices loaded with Mac and Windows software. Consider also adding **antivirus software** such as Total AV, Avast, or Norton on all devices.
7. Make sure all employees utilize **strong passwords** or, better yet, **passphrases**. 1234 is not a strong password. Using the names of children or pets in a password does not lead to a strong password, especially if you post on social media and talk about your dogs and children by name. A bad actor who steals your device will check your social media posts and use the information to deduce a password. Make sure to use a password on your phone or facial recognition.
8. Better yet, ask your vendors for help instituting **multifactor authentication**. Microsoft and Google (https://myaccount.google.com/signinoptions/two-step-verification/enroll-welcome?pli=1) software offer this option.
9. Institute a rule that employees **may not share** their password or passphrase with anyone, co-workers, or family members. Also, inform employees not to write down their password or passphrase and leave it lying around, such as on a post-it stuck on their monitor.
10. Institute a rule that employees **may not share** their devices with family members. If they must share, the family members should not be allowed to download games or apps on the work device, they may have malicious malware or other nasty software. Work devices are for work purposes, not a toy for family amusement.
11. Consider **backing up** all your records or at least critical documents on a separate hard drive or to a storage system in the cloud. In that way if your devices are compromised or you experience ransomware you have key records and documents stored separately so that you can try to avoid paying ransom and avoid loss of critical records. Back up regularly.
12. Keep **browser plug-ins** (Flash, Java, etc.) up to date.
13. If employees download documents and records onto **thumb drives** to work on them at home, they should make sure the contents are encrypted.

14. Train your employees not to be vulnerable to **phishing** and **random clicking**.
    a. Be suspicious of any official-looking email that asks employees to transfer **personally identifiable information** ("PII": social security number, birth date, bank account information) of members or employees or financial information of your council or congregation or that request a transfer of money outside your organization. Encourage employees to double check such official-looking emails with the sender (preferably in person or by phone) and encourage supervisors to give grace to employees asking if they sent them an email asking them to transfer funds or PII.
    b. Regarding transfers of funds, a safe practice would be that transfers of money cannot be ordered by email, rather, they can only be done by a request in-person or by a request on paper. Bad actors will make requests by email and will attach an urgency to the request to try and get an employee to act in a panic without thinking or questioning the request.
    c. If attachments or links in an email are unexpected or suspicious for any reason, do not click on them. **Do not click on links or attachments from unsolicited emails**. Ask family and friends not to send to your work email account links to videos of cute cats or stupid human tricks. Save them for your home email.
    d. Avoid visiting unknown websites or downloading software from untrusted sources.
    e. Only install apps from trusted sources (Apple AppStore, Google Play).

If you cannot accomplish these recommended steps all at once, take it step-by-step. If you need help, ask around. You might be surprised who in your council or congregation can help or who knows someone who can help institute these basic steps toward cyber security.