CORAC

FOR ALL EMERGENCIES: CORAC runs a HAM radio net and Signal groups. If communication goes out for any length of time, meet outside your local Church at 9 a.m. on Saturday mornings if it is safe to do so. Tell friends at Church now in case you can't then. CORAC teams will be out looking for people to gather in and work with.

Cyber Attack Scenario

ALL DEVICES ARE SUCCEPTIBLE

Cyberattacks are malicious attempts to access or damage a computer system and can lead to loss of money, theft of personal information, and damage to your reputation and safety. They can also block your access or delete your personal documents and pictures, and cause problems with services, transportation and power on a larger scale.

PREPARE NOW

- Keep your anti-virus software updated.
- Use strong passwords that are 12 characters or longer. Use upper and lowercase letters, numbers, and special characters. Change passwords monthly. Use a password manager.
- Use a stronger authentication such as a PIN or password that only you would know. Consider using a separate device that can receive a code or uses a biometric scan (e.g., fingerprint scanner).
- Watch for suspicious activity that asks you to do something right away, offers something that sounds too good to be true, or needs your personal information. Think before you click.
- Check your account statements and credit reports regularly.
- Use secure internet communications. Use sites that use "HTTPS" if you will access or provide any
- personal information. Don't use sites with invalid certificates. Use a Virtual Private Network (VPN) that creates a secure connection.
- Use antivirus solutions, malware, and firewalls to block threats.
- Regularly back up your files in an encrypted file or encrypted file storage device.
- Limit the personal information you share online. Change privacy settings and do not use location features.
- Protect your home network by changing the administrative and Wi-Fi passwords regularly. When configuring your router, choose the Wi-Fi Protected Access 2 (WPA2) Advanced Encryption Standard (AES) setting, which is the strongest encryption option.

LIMIT THE DAMAGE DURING

- Limit the damage. Look for unexplained charges, strange accounts on your credit report, unexpected denial of your credit card, posts you did not make showing up on your social networks, and people receiving emails you never sent.
- Immediately change passwords for all of your online accounts.
- Scan and clean your device.
- Consider turning off the device. Take it to a professional to scan and fix.
- Let work, school, or other system owners know. Information Technology (IT) departments may need to warn others and upgrade systems.
- Contact banks, credit card companies, and other financial accounts. You may need to place holds on accounts that have been attacked. Close any unauthorized credit or charge accounts. Report that someone may be using your identity.