BEWARE – SCAMS ARE ON THE RISE

In April, many of us received emails from an account using Pastor Kurt Wenzelburger's name. These emails were scam messages, but a number of people responded. Just a reminder that the best way to detect if the message is directly from our pastors or any other staff member is to check the source account to make sure it is coming from their St. Peter (@splcs.net) account.

In addition, we have heard personal stories of members receiving phone calls claiming to be the person's family member and asking for cash or gift cards. These are also scams.

Here are three ways tech support scam criminals target older adults:

- **Websites:** An unexpected pop-up window, often redirected from a legitimate website, may tell you that your computer is infected with a virus. This "ad" may prompt you to call tech support immediately using the number displayed.

- **Emails or text messages: T**ech support scam emails are made to look like they come from credible, recognizable companies. These messages can contain malicious links or attachments that send you tech support "alerts" when you click on them or open them. These fake alerts can actually freeze up your screen or keyboard to make you believe something is wrong with your machine. You may get e-mails from what looks like your utility company telling your account is in jeopardy. The utility companies will NOT be sending those e-mails.

- **Phone calls: P**hone scams are often run out of professional call centers. Scammers carefully choose vulnerable targets—like older adults or people with disabilities—and use proven scripts to drum up fear and anxiety in those they call. Posing as a tech expert, they may claim your computer has malware or other dangerous issues that must be addressed right away. They may request remote access to your system, which can allow them to install malware or steal your information. They also may pose as a family member needing help.

How do I stop tech support scams?

1. **Be wary:** Handle all unexpected, inbound communications with caution. Most reputable companies do not send out unsolicited phone calls, emails, or online messages. Real tech support departments will never ask you to pay with gift cards or a bank transfer.
2. **Be assertive:** If a caller insists there's an urgent problem with your computer, don't be alarmed—and don't be afraid to say "no" and hang up. If a caller claims to be from a reputable company, verify that company's phone number and call the number directly. If they demand money to help a family member, hang up and call that family member directly on their own phone. Never withdraw cash to "help them out".
3. **Be protective of your personal information:** Never give out your personal or financial information by email or by phone. When conducting online transactions, use credit cards instead of your bank info or debit card. Most credit card companies will not hold you liable for fraud, which makes them a safer way to buy online.

Helpful Websites: https://www.olderadultnestegg.com/ https://www.aarp.org/money/scams-fraud

*John 10:10 The thief comes only to **steal** and kill and destroy; I have come that they may have life, and have it to the full.*

Submitted by Paula Hoegemeyer, Parish Nurse