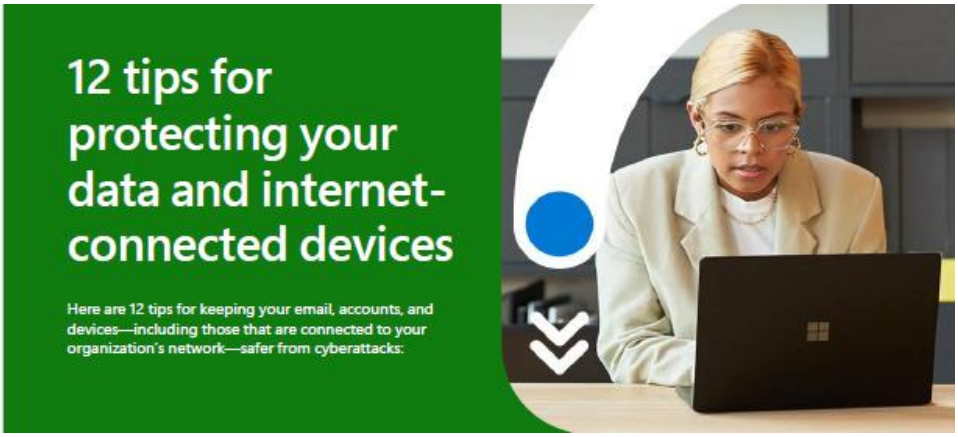

1. **Be skeptical of messages with links, especially those asking for personal information.** Fake links and websites can be very convincing. Rather than trusting links, find a phone number on the sender's official website so you can call them directly to confirm the message is legit.
2. **Don't trust the sender's name in an email you've received.** Display name spoofing is a type of email impersonation where cybercriminals make an email appear to come from a trusted source. This trickery often leads recipients into opening the email, clicking on malicious links, or revealing sensitive information. Look at the email address. If something seems off, don't open the email. Learn more here:
3. **Use branded email addresses for your organization instead of free email addresses from sources like gmail.com, yahoo.com, Hotmail.com.** Branded email addresses match your website's domain name. A branded email address will help separate your emails from spammers. Branded email addresses enable co-workers and parishioners to easily verify an email from you is legitimate.
4. **Be on guard against messages with attached files.** Never open unexpected attachments, even if they seem to come from people or organizations you trust. If you're concerned that the message may be important, **call** the sender to verify.
5. **When it comes to passwords, make them "strong and long."** Strong passwords have at least 14 random characters and symbols. Be sure to include both upper and lower case letters.
6. **Passwords should be unique.** Cyber criminals take advantage of the fact that many users reuse their credentials across various platforms. Cracking your password once, they can use that same password to gain access to other accounts.
7. **Enable the lock feature on all your mobile devices.** Require a PIN, fingerprint, or facial recognition to unlock your device.
8. **Only download apps from your device app store.** Only install apps from the official app store.
9. **Use Windows 11 and turn on Tamper Protection to protect your security settings.** Always use the latest version of Windows. Tamper Protection blocks unauthorized changes to your security settings.
10. **Keep your computer up-to-date.** Microsoft Windows Updates are an important for securing your computer but PC and Laptop vendors also regularly release their own updates meant to keep your safe. For example, HP provides "HP Support Assistant" and "HP Image Assistant", two small apps you can install that will scan your laptop and suggest important updates. Dell and Toshiba also have their own apps. Check your manufacturer for more information.
11. **Limit what you do on free/public WiFi.** Public wireless networks/hotspots are unsecured. Anyone could potentially see what you are doing while connected. Especially avoid logging in to key accounts like email and financial services. Consider using a virtual private network (VPN) or a personal/mobile hotspot if you need a more secure connection.
12. **Above all, stay alert:** Keep an eye out for things that don't look right. Watch for misspellings, double-check website URLs and look for pixelated or distorted logos. Also, be sure to ask yourself questions like "Why would this company need this information?" or "Would I normally get an email for something like this?"