Digital Awareness in 2021, The decade that led us from viruses to scams.

In taking care of the needs of a modern church office, the two big subjects are security and backups. As long as you have both, you should be in good hands.

1. Security/Digital Awareness

   With both PC and Apple computers having become so hardened over the last decade, with their built-in security, traditional viruses have become very rare. Still, and especially for peace of mind, it never hurts to have defensive software. For PCs, I would recommend Avira or Comodo Firewall on the free side or Malwarebytes on the paid side.

   The new term in our industry is “digital awareness.” This affects both Mac and PC users and is currently overwhelming the majority of current issues.

   When malefactors can no longer break into our devices, they shift to trying to get us to give our login info away… and have become very successful with it!

   What you will typically encounter is a phone call claiming to be from a trusted company, an email claiming to be from a trusted company, or a full screen pop-up on a trusted website telling you that you are infected and to contact Microsoft at the following phone number, etc. immediately. Here's how to fight these attempts, using fwepiscopal.org or chase.com as examples.

   A. Phone call: You get a phone call claiming to be from the Diocese or Chase. Only continue the conversation if they can send a confirmation email to you with an email address ending in @fwepiscopal.org or @chase.com. This also applies to the IRS, Social Security, Microsoft, or whomever. No matter how persuasive they may be, insist on receiving the email. This helps you identify a scammer.
   B. If you receive a suspicious email from Office365, apple.com, etc. saying you need to login using a provided link or your email/service may be disabled immediately, check the email sender’s address. If from fwepiscopal.org or chase.com, it will not end with @fw_episcopal.org or @chasebank1.com, as examples. It is very common for false login links to be sent from email addresses that are slightly wrong to appear legitimate.
   C. The full screen pop-ups that seem to lock your computer, telling you that you have a virus and to contact the IRS/Microsoft, etc. occur on both Macs and PC’s. They come from hijacked advertisements and are dressed/re-painted as false system messages, instructing you to call a number. Just hold your power button in until your system shuts down and reboot. Your system was not infected and you avoided the phone scam.
   D. Lastly, I highly recommend using either the Chrome or Firefox web browsers to surf the web. Both can use a downloadable add-on called Ublock Origin. This is a free add-on that blocks nearly all advertisements, including the scams, and works on every platform. You will have to search and download it, but that should take under a minute. Traditional antiviruses don’t block this content and this is a big area where malicious and misleading content comes from.

2. Backups – The other really important bit!
   In the age where our data is worth well more than the computers that house it, backups are key. While Windows Backup and Apple Time Machine are great ways to save a backup to an external device or additional hard drive/flash drive; it has become increasingly important to make sure your backups are also online. What few viruses remain, mostly "crypto viruses," aim not at taking your data, but encrypting it and demanding ransom payments. These encryption viruses can include your onsite backups. Many organizations have had to start over, despite having onsite backups.

   The recommendation is 1) you backup to another storage option than your computer, and that 2) you backup to an online service. I, too, am not totally excited about this but have seen it save many organizations. While Google, Apple, Microsoft, and others provide their own services, I recommend other services, such as Dropbox or Carbonite, that are not known to take "anonymous user data" from files backed up to their services. In effect, you can choose folders on your computer that you can "set and forget." This gives you the comfort of knowing that your current version of files and many previous, can be pulled either from the cloud or local backups.

In summation, make sure to be "digitally aware" and prepared for possible scams. Backup your data responsibly.

If you have any questions, feel free to reach out.

-John Campbell
Computer Systems Engineer