Evangelical Lutheran Church in America
God's work. Our hands.

Tips for Computer and Internet Safety

By better understanding security threats associated with the use of computers and the internet, and by understanding the manner in which these threats are exploited, you can better protect your congregation, your congregation's information, computers and computer files.
Every day, people are trying to gain unauthorized access to computers, applications, confidential information, and other valuable electronic assets all around the world. In some cases, the people trying to gain this access might even be known to you; some can be your co-workers or other people that you trust. Unauthorized access to computer resources can result in the loss corruption of vital information or damaged reputation of your congregation or people within it. These tips are not meant to cover all aspects of computer and information security, but are basic guidelines to begin to secure computers and information assets against common threats. The tips we will cover are in relation to the following topics:

Physical Security

Prevention against information theft best begins with securing the physical assets within your organization. Physical security refers to protecting the physical access to a PC, laptop, or server. Any other virtual security measures prove worthless if an ill-meaning individual is able to walk up to a logged-on system, shoulder-surf authorized users, or browse a laptop full of contact information and other unprotected data. There are several quick things that you can do to protect against this threat:

- Ensure you log off or lock your machine whenever you leave it unattended. A quick press of the Windows Key and L key at the same time will lock your machine before you walk away from it.
- The built-in screen saver on your mobile or computer offers the ability to automatically lock your system and require a valid password to access the system, should it remain unused for the period of time you specify.

- When traveling with a laptop, or smartphone, it's imperative that you keep these units within view at all times or secure with lock that attaches to any notebook or other hardware equipped with a lock slot. In the event that a portable system is stolen, the thief would be able to hack the unit at their leisure, potentially enabling them to assume your identity, access all your system's data, log on to the network, and access the organization's data.
- Ensure that your servers are kept in a secure location within your building that has restricted access. Flash drives are a quick way for thieves to steal data off of your servers or infect them with a virus or spyware.

Protecting your user name and password

When combined, a username and password create a powerful combination in allowing access to sensitive information. A username and password combination should be utilized to protect all personal and networked computers. The user name is the electronic identity providing the ability to log on to your PC or laptop, access network resources and data, surf the Internet, and send and receive e-mail. Paired with your username, the password is the key to your private digital assets - similar to the key to your home. Account names can often be guessed very easily, which makes protection of your password(s) even more critical and should be much more difficult to crack. Here are several tips to securing your passwords:

- Never provide your password to anyone.
- Never write your password on paper.
- Always create complex passwords to help prevent committed hackers from cracking them. Passwords should include letters and numerals, and when possible, special characters such as the pound sign (#) or ampersand (&).
- Try using phrases that are easy to remember – they should be longer than 14 characters.

  Avoid using passwords that include information based on:
  - Your name or username
  - Names of your spouse, children, or pets
  - Social security numbers
  - Anniversary or birth dates
  - Favorite sports teams
  - Words in the dictionary
  - Avoid using versions of these weak passwords by spelling them backwards or altering them by simply adding numerals to the beginning or end.

Adopt a Policy for Internet and Computer Use

Computers are used by synods and congregations for correspondence, bookkeeping, members' personal data, emails, website creation and research, as well as a variety of other important functions by staff and volunteers. It is important to safeguard the synods or congregations use of computers and the internet. One important step in this safeguard process is to adopt an Internet and computer policy.

A policy should be reviewed by the congregation council or committee for adoption. A policy needs to set forth for those authorized to use computers and the internet, and what uses are limited or prohibited. Any policy should make clear that computer and internet access are privileges; their use is not private and is subject to review at any time.

To aid you in establishing an Internet and computer policy, visit these links for sample policies for your consideration and review: PC/Network Agreement and NOREX contributed Information Security Policy. The first is a very basic sample that will also assist with tracking of computer based assets that are provided to various personnel. The second is a robust security policy sample from a member maintained by the ELCA Churchwide Information Technology Organization.

[Top]

Social Engineering

Social engineering is a tactic used by people to try to obtain information from you to use for malicious purposes. Social engineering attacks rely on a person's nature to trust people and to help one another when persuasively convinced that the individual requesting the information is well intentioned. These efforts to con you will include attempts to get you to reveal your account names, passwords, and other sensitive personal information. These individuals will often pose as customer service representatives or even IT support staff. This information will then be utilized to gain unauthorized access to systems and data. You should never provide sensitive account or personal information to anyone over the phone for which you can not verify who they are and where they are calling from.

A major reason for the increase in sales of paper shredders is due, in part, to one form of social engineering called "dumpster diving". Rifling through trash for account or personal information, has proved to be a very successful means for these ill-willed individuals to obtain this information about you.

Phishing

Phishing is a relatively new threat that has gained a lot of popularity lately in getting people to reveal sensitive information. Phishing relies upon purely electronic means to attempt to obtain this sensitive information. The most common method is an e-mail message that appears to come from the victim's bank, online store, or other financial companies. These fake messages typically state there's been a problem and the victim must click on a provided link and confirm or update account information. Victims end up submitting their account information directly to the scammer and thus compromise their identity.

Phishing attempts continue to improve and appear, at least on the surface, to be legitimate. They contain real company logos, apparently valid URLs and come from seemingly legitimate email addresses. The logos are typically stolen from the real company's web site; the URLs are typically redirected to web sites unassociated with the actual organizations, and the email address sources have been forged.

In order to avoid phishing scams altogether never provide sensitive, proprietary, or confidential information; or account, password, or financial information in response to an e-mail or instant message. Also, pay close attention to the address information for the web sites you visit. Always confirm that account or other sensitive information you provide is being entered on the proper organization's Web site and that you haven't been redirected to another location. Many phishing scams might include a URL that appears to be from yourbank.com, but instead directs to a fake Web site owning a suspicious or numeric URL. This is an immediate sign that you shouldn't provide any information.

Viruses & Spyware

Always remember – you should **not** click on unknown attachments received in unsolicited e-mail messages, particularly those from unknown persons and even on attachments received unexpectedly from people you do know. Often, individuals can be sending a virus in a file and not even know it. If you are ever in doubt, confirm that this person meant to send you a file, link or image in an email or instant message. If there is no way to confirm with the sender, then make sure to scan the file with any leading anti-virus application.

Never install programs found on unknown websites on the Internet; you should only download applications from trusted Web sites at home and use only authorized programs at work. In addition to viruses, spyware and adware programs may be contained in these downloaded applications. Spyware and adware are nuisances that will consume unnecessary system and network resources, potentially monitor everything that you do on your computer, and often report your behavior to advertisers or other third parties. This reporting can be in the form of confidential information, such as your bank account and credit card numbers.

Whether at home or at work, every PC and server should be configured to run Anti-Virus and Anti-Spyware software to scan new files as they are placed on your system, monitor changes to your system by newly installed applications, and scan all files on the entire computer at least once a week. There are several commercial Anti-Virus programs that are recommended for use from Symantec, McAfee or Trend Micro. For your personal computers, two free programs from AVG and Avast are also recommended for use. Popular antispyware applications include Lavasoft Ad-Aware and Microsoft Security Essentials.

You should be sure to check for periodic updates for both Anti-Virus and Anti-Spyware applications to ensure that your system is protected against all of the most current threats on the Internet.

Public Wi-Fi

While it is incredibly convenient, caution should be exercised when using public Wi-Fi. It may be an important and cost-effective method of gaining internet access, take note of the following methods of reducing risk:

- Choose your network wisely – If you are not at Starbucks, but you see STARBUCKS_FREE_WIFI, do not connect – it may be a fake/malicious access point.

- Make sure your computer is up to date with patches
- Forget the network – When done using public Wi-Fi, don't "remember" the network.
- Don't do financial or other business that is confidential in nature over public Wi-Fi

Always be suspicious of connecting to public Wi-Fi. It is getting easier for criminals to intercept Wi-Fi signals and to masquerade as legitimate Wi-Fi hot spots. When able, use the personal hot-spot functionality on your phone instead.

Using Public Computers

Public computers offer no guarantees of security or privacy of any information that is accessed while using them. This includes any email that you may have read, any credit cards that you used while shopping, or any passwords entered. You should only use public computers when absolutely necessary or for general web browsing. If you absolutely need to use a public computer to enter any sensitive information, do your browsing in "private mode" or "incognito mode". By doing so, this does NOT guarantee safety of information you entered, but is a small step to mitigate a few exposures of using a public computer. For more information on how to stay safe while using a public computer with Internet Explorer, please visit this web page provided by Microsoft.

Backups

Be sure to backup essential data on your computers. It is recommended that any critical files are backed up on a regular basis to protect against loss of data in event of a system crash. Considering the recent "ransomware" attacks, backup is an even more important component of your recovery plans in case of an attack of this nature. Backup software is included with all versions of the Microsoft and Apple operating systems. This can be used to protect your data by moving it to another computer, a set of DVDs, an external hard drive or a USB memory thumb drive. It's important to remember that someone should be checking that the backups are completing successfully. Nothing's worse than trying to restore data, to find that it didn't backup properly.

Network Security

Ensure that your IT group is properly managing network security. A security approach that leverages several layers is the most effective in protecting the computers and information that is stored on them. Firewalls, internet web filtering software, wireless network protection and several other technologies should be reviewed for applicability of use within your organization.