Mentor's Computer Security.

As a Lodge Mentor you probably have personal information about Candidates and new members on your computer. The following is some useful guidance About safeguarding this information from falling into the wrong hands.

The following guidance not only applies to keeping your Masonic data safe but equally important your personal data too.

Passwords

A familiar topic for Freemasons. Make sure your computer is password protected so that Unauthorized persons cannot start up your computer without the correct password. Also if using a screensaver, in the screensaver settings there is an option to require the Password to come out of 'screensaver mode'. This will protect your computer if you Leave it unattended for a short time. If your leaving your computer unattended for a longer period of time, then log off or switch it off.

User Accounts

For normal use log onto your computer using a normal user account, not one with administrator privilages, this way if someone does hack into your computer using your user account they will not be able to change any system settings. If you need to change settings you can log off and then log on as an administrator. Don't use the same password for both accounts.

Password protect files

Files such as MS Word documents, XL documents and Adobe PDF documents can be Password protected. See the help files in these programs for information on how to do this. You should consider password protecting documents containing personal or Confidential information about members.

Memory sticks are now freely available at all computer shops and plug into your computer’s USB ports. These are essentially removable drives and act just like An extra hard drive when plugged into your computer. In addition to the steps above,
Consider saving your password protected documents onto a memory stick. This has the advantage that you can carry it with you and the files are not on your computer.

Keeping up to date

It goes without saying that everybody who uses a computer should have good anti-virus software installed on their PC and laptop. It is equally important that you keep this software up to date. Most good anti-virus programs have a built-in auto-update function which will automatically download all the latest virus definitions to keep your computer safe. However, to do this your computer has to be switched on long enough for the update to initialize, download and install. there was a case recently when someone got a virus on their computer even with good anti-virus software on board. The computer in question was a laptop, but this advice applies to all PC’s. It turned out that the owner was in the habit of leaving his laptop switched off and only switching it on long enough to check emails and then he switched it off again. Not long enough for the laptop to do its’ anti-virus update but long enough for it to get infected from an email he had opened. So my advice is this, if you do not leave your computer on for any significant length of time, whilst using it click on the anti-virus icon and update the definitions manually. The same applies to Windows updates which are equally important in protecting your computer. However, if your computer is on all the time or for several hours, the updates should occur automatically. But, if in doubt, do the updates manually.

Virus Threats

It has been estimated that in normal web surfing and usage it only takes between 5 and 15 minutes for an unprotected computer to become infected with some kind of virus or malware. So what can you do?
Emails:

- NEVER open an email attachment from someone you don’t know.
- NEVER ignore a virus warning or system warning thinking you know better.
- If you are in any doubt about an attachment you have opened carry out a full virus scan to be safe.
- NEVER answer any email purporting to come from a bank or similar institution asking you for any personal information or warning you that your account has been hacked/accidentally deleted or any other reason. This is called phishing and the senders are trying to trick you into giving them your personal information.

Usernames & Passwords:

NEVER use the same username and password for different email or other online accounts such as eBay or PayPal and include letters, numbers and symbols in your password as this makes it very much harder to crack.

Web Surfing:

It has been estimated that approximately 18% of all websites on the internet are infected with some form of malware including viruses. If your browser is up to date the chances are it will pick up the threat and warn you. You may get the option to proceed to the site anyway. Again unless you are sure the site is safe then do not go there.

Google and other Search Engines:

Malware sites often have names similar to well known and popular websites such as Gooble instead of Google. When you do a search for Google, the Gooble site will appear on the list and people sometimes will click on the wrong site on the list because they are not paying full attention and will be taken to the dangerous site where their computer will be infected very quickly.

Real and Hoax Threats:

There are very many real viruses out there in the wild. There are also as many hoaxes out there too. As well as keeping your virus checker updated from time to time, you should go onto the website of your virus checker and check the latest news. This is the only place where you can be sure the information is accurate.

NEVER take at face value any email which tells you that unless you send it to EVERYONE on your contacts list all sorts of nasty things will happen…you just have to do one thing, send it to the recycle bin. The sender has probably thought he has done a good thing by forwarding it to you as asked, but he is wrong for the following reasons:

- The information is probably false and the accuracy of its contents was not checked before forwarding it.
- If there happened to be some malware on the senders computer it would have sent a copy of the email to its creator thereby giving him all the email addresses on the list.
- Most importantly, this type of activity, with everyone sending the warning to everyone on their contact list increases internet traffic exponentially and slows the whole internet down, especially email servers, which was the intention of the author of the hoax in the first place.

So if you get such an email bin it and let the sender know so they don't send it out to anyone else. If you not sure if the warning is valid or not, do your own research using the email's header as the Google search criterion.

District Grand Lodge of Cyprus

Updated June 2019