(Approx. 1037 words)

## Personal Computer Security

By Dick Maybach, Brookdale Computer User Group

www.bcug.com

n2nd (at) att.net

Home users must manage three types of security:

* information security – protecting their information,
* application security – securing their applications against modification and misuse, and
* network security – preventing access to their network.

Only a small portion of your data, such as passwords and credit card numbers, is sensitive and needs special protection. For most, you are concerned only with recovery if lost, and here a good, well-tested backup discipline is the solution. It doesn't matter if the loss was because of hardware failure, operator error, or malicious software. Please note the "well-tested." If you haven't recently and successfully restored data from a backup, you don't have a backup discipline, only a backup hope.

Sensitive data must be encrypted. I use KeePassXC, <https://keepassxc.org/>, for passwords, PINs, and financial access data, such as credit card and bank account numbers. The program stores these in an encrypted database, which I keep on my PC. If you keep it on the cloud, it will be available to all your devices with Internet access, but it's also more vulnerable to attack there. This means it needs a stronger password. A compatible Android app uses the same database as KeePassXC, which means the data is also safeguarded on your smartphone. The application also generates passwords of arbitrary complexity, making using a unique, strong password for each account easy. Other password programs have similar features. I use VeraCrypt, <https://www.veracrypt.fr/en/Home.html>, to encrypt files, directories, and storage media on my PC. I've seen reports that the EDS app allows access to VeraCrypt files on Android, but I haven't tested it.

Many financial institutions require two-factor authentication when you access your account. The most common is texting a one-time PIN to your cell phone after you log into your account with a username and password. You need both your password and the registered smartphone with them. Also, be careful when you travel that you can receive text messages in the countries you visit if you use credit cards.

Phishing attacks, where you get calls or messages asking you for sensitive information, are far more common than those through your PC. I get these almost every day, such as:

* "Your bank account has been locked; click this icon to unlock it,"
* "Your email storage is full; click this icon to free some,"
* "Your PC is infected with viruses; click here, and Microsoft will help you solve this,"
* "Amazon is about to ship you a new cell phone and charge your account; click this icon to prevent it," and
* "You owe money for past-due taxes; call the IRS at this number."

Usually, these are obvious scams, but occasionally you must do something. For example, your credit card company may contact you about a questionable purchase. In such cases, log into your account with the contact data in your password file or call the number on the back of the card. Also, never use a link in an email.

Many attacks occur when you contact disreputable websites. However, you can protect yourself by improving your browser's security.

* Chrome – <https://support.google.com/chrome/answer/10468685>
* Edge – <https://www.makeuseof.com/guide-to-security-settings-in-microsoft-edge/>
* Firefox – <https://trendoceans.com/firefox-privacy-and-security/>

Browsers are becoming more secure, which means keeping yours up to date is especially important. However, browsing can be dangerous; you feel safe because you are comfortable in your own home, but you are poking through the back alleys of the world. If you have any concerns, use the Tor browser, <https://www.torproject.org/download/>, to protect yourself. Even better, install Tails Linux, <https://tails.boum.org/>, on a memory stick and explore from there rather than your usual operating system.

Be careful where you obtain software. Years ago, we would go to a tech store to buy a box with the storage medium and a manual, but the stores, boxes, media, and manuals have all but disappeared. We now download or install it directly from the Internet. I prefer to obtain mine from its developer's website after verifying that the URL is valid, and the developer is reputable. I've learned to avoid sites that warehouse many programs, as their downloads often include unwanted extras or malware. Check any download for malware before you run it, and if possible, test it on a secondary computer or virtual machine before you install it on your primary PC.

Keep all your software up to date, not just the operating system but all your applications. Many have bugs, some of which have security flaws, and anti-malware software may not protect you from someone exploiting these. Delete those applications you no longer use, as every one you have installed is a potential security risk. This also applies to smartphone apps.

Internet Service Providers (ISPs) are notorious for not updating the software in their terminal equipment. Unfortunately, your home network may not be secure, which can be problematic, especially if you have local file servers or other network devices. You can reduce your risk by installing your firewall between your home network and the ISP hardware, providing that you keep it updated and properly configured.

Some companies promote Internet-of-Things devices, such as video cameras that allow you to check on your home from work. Unfortunately, not all are designed for good security; others can also check on your home. Always change the usernames and passwords of such equipment from their defaults. Consider carefully whether the convenience of these is worth the risk, and purchase only those for which you can find thorough valid reviews.

Using a laptop on a public hotspot is much riskier than using one at home, as all your Internet data packets are visible to others using the same hotspot. Be sure to set your PC firewall for this environment and use a Tor browser or a VPN to encrypt your packets. Of course, encrypting sensitive data on a laptop is even more critical than on a home PC, as laptops frequently go missing. They are also more easily damaged, so they should be backed up, preferably by storing that data remotely. All this is even more true for smartphones.

Some PC users think that security begins and ends with anti-malware software, but reading the above should convince you otherwise. Such programs are helpful but address only a small portion of the risks.