Online Security, Privacy, & Avoiding Problems

© 2014 by Scott@arxcomputers.com (847) 962-4661

"Distrust and caution are the parents of security." – Benjamin Franklin

We see the same computer problems every day. This is a short guide explaining how to avoid them and reduce recovery time and expense should your computer fail.

1. Rules for secure passwords and how to manage them
2. Spam and phishing emails
3. General guidelines on reducing hardware problems and solving problems
4. Best practices to reduce hardware and software problems
5. How to avoid spyware/viruses
6. Which updates to install
7. Tips on backing up your data

PASSWORDS

Many people think an 8 character random password like "h6yr73s4" is secure. They are sadly mistaken and countless email accounts with similar passwords are hacked every day. Here are the three golden rules for a secure password:

1. Twelve characters or more
2. No dictionary words
3. At least three of the four categories of upper case letters, lower case letters, numbers, and special characters like !@#$%

The best way to manage your passwords is an Excel spreadsheet on your main computer, hopefully one which does not travel (not the laptop that goes back and forth to work!). This is easily backed up, printed out to hard copy, and stored offsite, for example in a safety deposit box. You do not need to be an Excel expert to make this spreadsheet, and a Word document would be fine if you prefer. You need four columns – vendor name, username, password, and notes. Notes would be for account number, security questions, etc. By the way, your security question answers can be gibberish, as long as you write them down. The street you grew up on does not have to be answered accurately. It can be "f5G65!#ghs0sxz!"

- I personally don't trust the online password manager programs and I don't recommend keeping all your passwords on mobile devices like smartphones or tablets.
- You do not need to change your passwords regularly, just when requested by vendors if they get compromised, as eBay was in early 2014.
- Your financial passwords should be unique, but it is acceptable to keep some low importance passwords the same.
- You can change your password in the "My Account" or "My Profile" section of most web sites after signing in.

SPAM AND PHISHING

Spam email just means unsolicited commercial email. It falls into three categories:

1. Ads from legitimate companies – If you have purchased anything online, you noticed that the vendor, such as Target, puts you on its email list for advertising weekly specials. You can click "Unsubscribe" on the bottom of these emails and they should stop.
2. Ads from random spammers – If you don't recognize the sender and the contents include a link to a random seeming web site, delete the message. Do not click "unsubscribe." If you use a smart email service like Gmail or Outlook.com, you will not see very many of these emails.
3. Phishing – The most dangerous emails are phishing emails, which pretend to be from a legitimate company but are really trying to trick you into clicking on the link and giving them your username and password. If you are not paying attention, it's easy to fall for this sort of email. A good way to avoid this is to follow an important rule: don't ever click on a link in an email. If you get an email from Chase bank asking you to click on something, open your web browser and go to chase.com and sign in there. Opening the web site manually instead of clicking on the link in the email will keep you safe.

GENERAL IDEAS

1. Replace all computers every 4 or 5 years. Computers slow down over time, and are more prone to problems as they age. When we install a new computer for someone who has an old, slow machine, they always say they wish they had done it sooner. Imagine a 4-5 year old computer to be a 10 year old car.

2. Use popular software, as it has support available for common problems. If you have a problem with Microsoft Word or Excel, there are literally millions of web sites about the products and odds are hundreds of thousands of people had the same problem. If you use a niche product no one has heard of, there will not be much support available. Also, upgrade this software to the latest version every 4 or 5 years, usually when you purchase the new computer.

3. Keep data (documents, spreadsheets, pictures, music, etc) in one place on one computer, not 10 places on multiple computers. Then back that data up!

4. Save your installation CDs, product keys, serial numbers, codes, order numbers, logins and passwords for every program you install or purchase on the computer. The most important one is Microsoft Office (Word, Excel, PowerPoint).

5. When you see a strange error message, look it up on Google. I have been repairing computers since 1999 and I see a new error every day, which I then look up on Google. Because I am looking up errors with popular programs, the solutions are readily available on the Internet.

SPYWARE AND VIRUSES

Spyware is by far the most common problem we see. "Spyware" simply means advertising software. The symptoms include changes to your web browser home page, and repeated popup windows and warnings claiming that you're "infected" and trying to sell you their bogus products. There are no programs which will prevent spyware. The only way to prevent it is to be very careful where you go on the Internet and what you click on. Don't try to download music, movies, and games for free. Those programs can be packed with spyware.

The safest browser is Google Chrome, free from http://www.google.com/chrome When you're browsing the web and get a popup with dire warnings about how infected your computer is, close the window – it's a scam. If you're browsing the web and something tries to install itself on your computer, don't click yes or OK – close the window or restart your computer if needed. Be very skeptical of warnings and free software on the Internet. Should you be infected with spyware, call us and we can clean it up.

Real viruses are written by bored teenagers in their basements and are pretty rare. The antivirus program to use is the free "Microsoft Security Essentials," which has been renamed "Windows Defender" in Windows 8. Read our free guide on our web site (http://www.arxcomputers.com) about how to install it if you have Windows 7, click by click. If you have Windows 8, remove your trial antivirus from your computer, restart, and Windows Defender should activate automatically.

A "firewall" sits between you and the Internet and keep hackers out. Windows XP, Vista, and Windows 7 all have built-in firewalls that are user-friendly and work well. If you have any computers that connect wirelessly or have more than one computer in the house online, you also have a "router," which has a great firewall built in which will stop 99.99% of all hackers cold. You do not need to purchase a third party "Internet Security" or firewall program.

Viruses are also occasionally sent through email accounts and Facebook messages, both as attached files and as links to infected web sites. If you get an email from a friend or family saying "check out my vacation pictures from Paris!" and you know they haven't traveled recently, you should delete the email immediately and contact the sender. Their account probably got hacked because they didn't use a secure password.

The bottom line on avoiding spyware and viruses on the Internet is to be skeptical and cynical of popups, advertisements, and warnings. If you get a popup saying your registry has thousands of errors, close it. It's just an advertisement. If you get an email from the IRS saying you overpaid your taxes and please fill in your information for a refund, alarm bells should be going off. If someone purporting to be from Microsoft calls you on the phone out of the blue and wants to connect to your computer, hang up on them. This is a common scam.

UPDATES

Computers nowadays require a constant stream of updates. They are a bit tedious at times, but they're free and fix bugs and vulnerabilities. The first important update process is "Windows Update." Windows is the "operating system" of your computer. Like all software programs, there are weaknesses and problems discovered all the time, for which Microsoft releases free updates (also called "patches") to fix. Any recent computer should automatically install them regularly without much baby-sitting. This is why your computer occasionally says

"configuring updates" when you restart. You will not receive notices or links to updates in your email – ignore those fakes.

After many updates are released over 18 months or so, Microsoft bundles them up in a big package and calls it a "service pack" and asks permission before installing. I recommend that most cautious people stay a year or so behind the latest service pack due to potential problems. Windows 7 computers should have Service Pack 1 installed. If you have a Windows 8 computer, Service Pack 1 is being called "Windows 8.1" and I recommend installing it if you have not done so. To check your Windows and service pack level, right click on "Computer" or "This PC" and left click "Properties."

Some other important programs to update include Adobe Flash player, Adobe Reader, and any programs you use frequently, such as iTunes. These programs will pester you by asking permission to update themselves regularly. When allowing them to do so, watch out for extra programs you didn't ask for. There may be checkboxes which are checked by default, offering programs unrelated to the updates, which do not need to be installed.

In general, updates can cause problems on a rare occasion. This is normal, but you should install updates for the programs listed above anyways, as the alternative is burying your head in the sand and not fixing potential security vulnerabilities and bugs. You can safely ignore updates for HP or Dell software, as they are not security-related. If your printer is working, don't install any updates, as you will risk breaking it.

BACKUP

Even if your machine is clear of viruses/spyware and software is up to date, the "hard drive" which holds all your data can still die at any time, regardless of brand, size, or age. It's like your car breaking down. It can happen to a brand new Porsche or a 10 year old Toyota. Your laptop could be lost, stolen, or dropped. If you have any important documents, music, pictures, and any other files, you must back them up on a regular basis.

"What should I back up?" What would you miss? A good place to start is your Documents, Music, Downloads, Desktop, Favorites, and Pictures folders. Most email is webmail these days, so you do not need to be concerned with backing up mail and contacts.

"How do I back it up?" The basic idea in backing up is to copy data from your computer to another place: a USB flash drive, an external hard drive, online, etc. The most popular backup option is using an external hard drive. If you need help purchasing or setting this up, let us know and we can help. Our favorite brands are Western Digital or Seagate and you should buy a minimum of 2 "terabytes" of storage space for under $100.

Windows 7 has the ability to back up your entire computer to an external hard drive every day automatically. To easily set this up, click on *Start → Control Panel → Back up your computer*. Windows 8 has a great backup feature which can be easily activated by clicking on *Windows Key-X → Control Panel → File History*.

Another popular method of backup is online backup. There are many vendors, but our favorite is iDrive. Call us for help setting it up. The regular price for online backup is $5 per computer per month or $50 per year.

If you implement these suggestions, your chances of a major computer problem such as spyware or data loss will be drastically reduced. If you have any problems or questions, feel free to call me, Scott from ARX Computers, at (847) 962-4661. There is no such thing as a stupid question (but they're easier to answer).