Computer Bytes – December 2015

Provided By: Harv Oliver, HANDS-ON Consultations

Hello friends and associates – Happy Holidays! This session I want to visit security, in a different fashion, more directed to 'protecting your security'. It's an ongoing problem worth attention and vigilance.

One of the most common scams in today's world is you receive a call from someone stating they're from MICROSOFT. This really freaks people and in truth, lends an air of feeling secure - hey, if it's MICROSOFT, it must be legit. **IT IS NOT!** MICROSOFT will not call you! I myself have been hit up by these scammers and I've had a number of clients call and ask about validity. Unfortunately, I've also had some calls from those who were pulled in… This is just one example of a number of scammer issues we all must deal with. Here at ***HOC*** we can always help with the fix on the PC side but your other secure activities, bank accounts, credit cards, etc. are another story. At least for the PC side, let's reference some solid working procedures. Sure – we've heard most of this before but it's never a bad idea to revisit. Here we go…

1. **Never open unsolicited e-mail.**
   Always delete unsolicited e-mail and never click on a link in an e-mail from someone you don't know. Doing so could infect your computer with a virus. My other common advice phrase is 'when in doubt, delete!'.
2. **Use strong passwords that are impossible for a thief to guess.**
   Use a different password for each login, and make sure that each password is a combination of upper- and lowercase letters, numbers, and symbols. Yes, it's a pain but the best practice to be secure. People who use the same passwords for everything make it easy for thieves to steal their identities. P.S. Don't absentmindedly slip either and share 'oh, it must be this password as I use it for everything.' Don't laugh, I've heard this before! If you find it difficult to manage, there are tools that let you keep the different passwords but manage with one very secure password.
3. **Don't let your browser 'save' password for sites with sensitive and/or secure information.** You know the prompt I'm talking about, you enter login and password at your bank and it prompts 'would you like to save password?' Don't!!! The minor annoyance of having to enter is much less than the aggravation of being compromised.
4. **Install antivirus software and keep it updated.**
   There are many good antivirus programs online that people can download free or that you can purchase as needed. Review, compare, and find a fit that's good for your environment.
5. **Protect your computer with a firewall.**
   A computer firewall creates a virtual wall between your computer and thieves who want to access your personal information. Hardware (routers, etc.) and software firewalls help keep your computer safe when you're online. Microsoft has a built in software firewall or again you can purchase enhanced tools, software and/or hardware.
6. **Don't share your personal information online.**
   Social networks are fun and great for connecting with friends, but there are those who use them to trick people into providing their personal information . You wouldn't share your private information with a stranger on the street, so don't share it with a stranger online, no matter how long you've "known" them.

7. **Keep your operating system updated.**
   When your computer operating system tells you an update is available, update it as soon as possible, particularly if you note they are “security updates’. This suggestion provided, you do want to be sure the updates will not affect any applications or features you use that may not play well with some updates.
8. **Be wary of fake antivirus notifications and other scareware.**
   Antivirus viruses or malware trick users into thinking that they have a computer virus in order to frighten them into providing their credit card information to download an "antivirus program" that will remove it. Remember to never provide any personal information in the pop-ups that appear on your screen.

Let’s be truthful, nothing is 100% but we can avoid many problems by being attentive and sensible. And if you do get bit, don’t be embarrassed – it happens. Get help and get the problem taken care of ASAP to avoid continuing issues.

Once again, have a wonderful Holiday Season – talk to you next year!

NOTE: Our sharing of information within articles includes suggestions and tips. USE AND/OR APPLY AT YOUR OWN RISK. If you have any questions or concerns, please contact our offices for professional service/guidance.

Until next time, don’t forget your backups! For more information, contact Harv Oliver, HANDS-ON Consultations, (805) 524-5278, www.hocsupport.com