COMPUTER concepts

ONLINE SAFETY EXCERPTS

Excerpts and Links to Helpful Security Tips

BY COMPUTER CONCEPTS, LLC

September 22, 2011

The topics below are excerpts taken from Microsoft Online Safety web site. Each link takes you to the specific topic page and contains very important computer security information that you should be aware of.

This security information is very valuable, but too lengthy to include in any of our current class offerings. However, some of the topics will be discussed in Internet Security Essentials class.

Check your password — is it strong? - Your online accounts, computer files, and personal information are more secure when you use strong passwords to help protect them. This page allows you to enter your current password to see how strong it is relative to other strong passwords.
https://www.microsoft.com/protect/fraud/passwords/checker.aspx?WT.mc_id=Site_Link

Create strong passwords - Strong passwords are important protections to help you have safer online transactions.
http://www.microsoft.com/protect/fraud/passwords/create.aspx

Five tips to help keep your passwords secret - Treat your passwords with as much care as you treat the information that they protect. Use strong passwords to log on to your computer and to any site—including social networking sites—where you enter your credit card number, or any financial or personal information.
http://www.microsoft.com/protect/fraud/passwords/secret.aspx

How to recognize phishing email messages or links - Phishing email messages are designed to steal your identity. They ask for personal data, or direct you to websites or phone numbers to call where they ask you to provide personal data. A few clues can help you spot fraudulent email messages or links within them.
http://www.microsoft.com/protect/fraud/phishing/symptoms.aspx

What is the Microsoft Lottery scam? - The Microsoft Lottery scam is a fake email message that claims that the recipient has won the "Microsoft Lottery." **There is no Microsoft Lottery. If you receive this kind of email message, it has been sent by cybercriminals in an attempt to steal money from you.**
http://www.microsoft.com/protect/terms/microsoftlottery.aspx

Avoid Advance Fee Fraud and other lottery scams - Lottery fraud and frauds like Nigerian Letter are one of the fastest growing forms of Internet crime and costs consumers around the world millions of dollars every year. Advance Fee Fraud or lottery scams are fraudulent e-mail messages that come from someone you do not know or come from someone impersonating someone you know. The e-mail messages may also appear to come from corporate executives or government officials who are promising gifts or supervising financial transactions
http://www.microsoft.com/protect/fraud/phishing/mslottery.aspx

How to recognize spoofed Web sites - ***Spoofed Web sites are commonly used in conjunction with phishing scams. The*** spoofed site is usually designed to look like the legitimate site, sometimes using components from the legitimate site. Cyber criminals also use Web addresses that resemble the name of a well-known company but are slightly altered by adding, omitting, or transposing letters. For example, the address "www.microsoft.com" could appear instead as micosoft.com or mircosoft.com. ***This is called "typo-squatting" or "cybersquatting." Scammers register these domain names in order to compete with the popular site or to earn money through advertisements.***
http://www.microsoft.com/protect/fraud/phishing/spoof.aspx

Dick Smith, Director or Training
dick@ccwilliamsburg.com