Zēbis

Data Protection Tips

1) Erase sensitive data from your computer. Instead of deleting data that you want to permanently remove from access, utilize software that will allow you the option to delete or erase data.

2) Know that if you are a small-medium business and/or residential computer user, you are subject to non-discriminating automated attacks to gain private, personal information.

3) Understand keyloggers, how they work, how you may come in contact with them and how to protect yourself. (See separate handout.)

a) Public computer: do not enter any private information, ever.

b) Personal computer: isolate your computer from others at your office or home via a separate internal network.

c) Be on the lookout for web site scams that allow the downloading of keyloggers.

d) Avoid using insecure software such as Internet Explorer and Safari.

e) Set in place a robust hardware firewall.

4) Guard your computer from physical theft at public places including airport check points.

5) If you store sensitive information on your computer utilize a strong encryption program.

6) Avoid saving passwords for banking, PayPal, etc. web sites in your web browser.

7) Use strong passwords for access to important web sites and information. "Strong" includes numbers, symbols, upper and lower case letters.

8) Use fictitious answers for security questions.

9) Do not give in to "phishing" schemes. Know that reputable companies will not request personal information via e-mail.

10) Be careful when you are redirected to another web site. Verify that you are at the site you want.

11) When using off-site storage or cloud computing, encrypt all data or do not store sensitive data on those servers.