Computer and Network Security Presentation

ALPINE
BUSINESS SYSTEMS, INC.
There is no expectation of privacy on the Internet.

The only way to be totally secure is to stay un-connected to anything.
What Apple, Google, AOL, MSN, Facebook, your ISP, and the government know about you.
2007 – Self morphing viruses

2009 - The Zeus virus – “Man in the browser” attacks – no browser is safe

2011 – 300% increase in cyber –attacks
The perpetrators

- Who they are
- Why they do it
- Who are the targets
Spam

- Our filter processes 3 billion emails/day and 98% are SPAM.
- Easy to create, spoof addresses (impersonate someone else).
- Designed to decrease productivity, spread malware.
- Used by the spammers as a way to communicate.

Spyware

- Hundreds of attempts foiled every week.
- Designed to steal information.
- Multiple methods of infection – emails, web sites, music sharing sites.
Viruses and other Malware

- Thousands caught in our filter every day
- Designed to destroy or manipulate data, computers, networks
- Multiple methods of infection – emails, web sites, music sharing sites
“Drive-by Infections”

1 in 8 web pages are infected (Google statistic)

Be very suspicious

Always look for the name right before .com or .org in the URL
Phishing techniques

- Web Searches, E-mails or IM’s impersonating a trusted entity
- Directs you to a phony web site, then look out!
**Social Networking Sites**

- Facebook, Twitter, Google+, Pinterest, thousands of them
- The good, the bad, and the ugly
- Once it is on the Internet — it never goes away!
Smartphone Apps

Wall Street Journal – more than 50% take your personal info

Why Apple does not allow Java, Flash, etc.
Great technology if they are secured; Hacker’s paradise if not

Do not broadcast the SSID

Use encryption: WPA-PSK or stronger
Social Engineering

“The act of manipulating people into performing actions or divulging confidential information.” – Wikipedia

The latest and often the most effective tool

Some scenarios – the help desk, the acquaintance, the researcher
Lock your computer: CTRL-ALT-DEL – Lock Computer

Logoff your computer: Start – Shutdown - Logoff

Do not leave passwords written next to computer

USB Flash Drives – Cell Phones – Smart Phones

Notebook computers – one of the largest data theft targets
Logical Security

- Change your password regularly – CTRL-ALT-DEL – Change Password

- Minimum 6 characters; 3 of these: Upper, Lower, Numbers, Symbols

- Don’t give it to anyone – no matter what they say!

- Never e-mail work products to your personal e-mail account

- Meta-data- What it is, what is the risk
Home Networks

- Always use latest Anti-virus (ESET NOD32, Symantec, MacAfee, TrendMicro, Panda)
- Keep PC’s updated with Service Packs, Patches, Upgrades
- Never plug directly into Cable/DSL/FiOS modem
- Always use a router (Linksys, Netgear, D-Link)
- Use Network Address Translation and DHCP (standard defaults)
What you can do

- Never use your work computer for personal use
- Never divulge any information to anyone you don’t know
- Always convert to PDF
- Change your password regularly to a strong one (see Logical Security)
- Stop using “free” music/video sharing sites
- Lock or logoff your computer
- Report anything that is suspicious
- See advice above - Wireless and Home Networks
- Download and configure Trusteer Rapport, the anti-keylogger from www.trusteer.com