“We’ve been Hacked!”

Almost

Colin Arnold

Director of Academic Affairs

National Cyber Partnership • www.national-cyber.org

First some legal stuff

This is a brief overview of physical and cyber security in the workplace. This is by no means an exhaustive exploration of either topic but rather a presentation to get you to think a little differently about security. Please see your facilities coordinator to determine local safety and security measures (translation: we have no idea where the fire exits are).

CyberStudies Consortium

Nature of modern attacks

Whose job is security?

- CEO
- CFO
- Receptionist
- Janitor
- YOU!

Security is the job of EVERYONE!

Know WHO to report security issues to

- ALWAYS report issues in writing (email)
- Do not be shy about reporting (no one was ever fired for good security)
- Good idea to report issues to more than one person

Locks were made for a reason

Just say no to Facebook at work

- Stay off Social Media at work or when using company resources unless you want EVERYONE to know your business
- Stay off the Internet (unless it is part of your job) and only go to approved sites if you do have to go on the Internet
- 39% of all hacking and malware attacks occur through a web browser (source: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf)

Don’t be these people…

CyberStudies Consortium

Personal Devices Usage Policy

- Do not connect your phone, tablet, fitbit, iPod, Smart Watch, personal laptop or anything else to company resources without explicit permission to do so.

CyberStudies Consortium

NEVER share your password!

- Not with IT
- Not with your boss
- Not with your co-worker
- Not with your spouse/partner
- Your password is tied to your account which is tied to activity on the network. Don't get held accountable for someone else actions with your account!

Don’t write down your password

- Bad guys look for a written password as soon as they get physical access to your space.

- Bad guys don’t always look like bad guys–cleaning people, plant wranglers, the intern, electricians, plumbers, etc.

CyberStudies Consortium

[c]0mp13x p@55w0rd5

- Use passphrases instead of a password, longer are harder to crack
- Use "leet" translations and not just words but combinations of upper and lower case letters, numbers, special characters and even spaces!

Some "leet" translations:

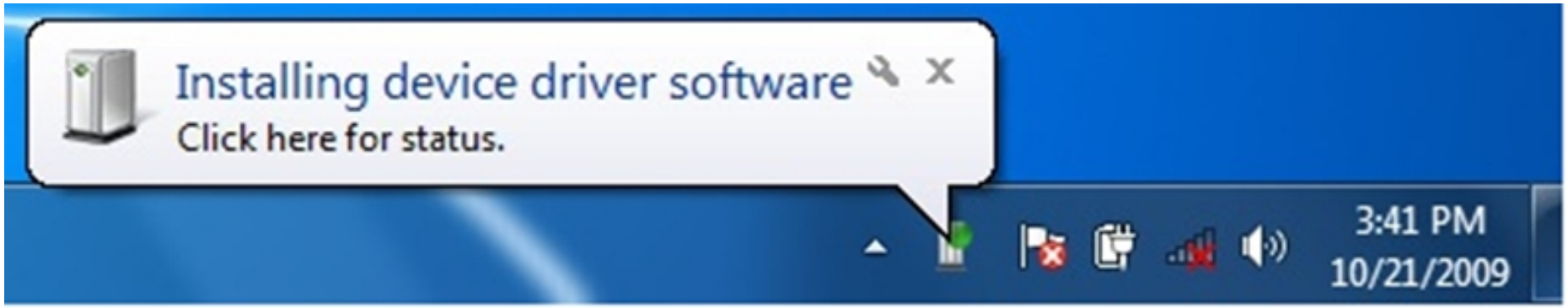
a=@ c=(e=3 g=6 h=4 i=1 OR i=l L=1 o=0 s=5 t=+ so "password" becomes P@55w0rd and becomes about 42 million times harder to break! (But P@55w0rd is well-known, so choose something else.)

A passphrase using leet translations looks like: iG02publiX4f00d

The “found” USB drive

- Never, ever, ever plug in a USB drive, play a CD or DVD or plug in any device capable of carrying data without first having it cleared with your IT department!

(look familiar?)



CyberStudies Consortium

#1 tool for hacking? **PHISHING**

- Favorite tool of the Chinese, Russians, North Koreans and other nefarious criminals
- Lures (<-hence the name) the victim into clicking a link that infects their computer, usually via email
- Email often looks like it came from a legitimate source
- STOP Phishing with one word!

If it looks suspicious, it probably is!

- It is OK to question whether someone is from IT or not, or if they are truly part of the executive team or a board member.
- No one has ever been fired for good security
- Your security has to be perfect EVERY time, but the bad guys only have to get lucky once

In closing, remember 4 things

- Report ALL suspicious activity to your direct supervisor and probably at least one other person (in writing).
- DO NOT talk about work or the technology you use at work with ANYONE.
- It is OK to be paranoid. Paranoid people stay employed longer ☺
- EVERYONE needs to be trained and PRACTICED

Colin Arnold

Director of Academic Affairs, National Cyber Partnership

carnold@national-cyber.org • www.national-cyber.org

CyberStudies Consortium