Chemeketa Community College

Center for Cybersecurity

Welcome to the Center for Cybersecurity at Chemeketa Community College located in Salem, Oregon. Chemeketa has developed a Cybersecurity Center to provide access to Information Security and Information Assurance resources.

Contact Info

Mandy Reininger
CIS Instructor
Salem Bldg. 37, Rm. 131
503.365.4822
Email

Don Kraus
CIS Instructor
Salem Bldg. 37, Rm. 126
503.589.7687
Email

Cybersecurity Associates Degree

News and Events

Resources

Faculty
What’s to come...

In the following slides I am going to discuss amongst other things and in no particular order things to enlighten, frighten, educate, and hopefully . . . inspire you to stop being apathetic about security so that you, can use the internet with greater confidence and safety.

I will recommend specific technical solutions for improved protection of personal data assets.

Identify security and privacy risks.

Identify the best means of avoiding or mitigating threats.
Cyber Security Basics

Protect Yourself
Because no one else will do it for you.
PROTECT
AVOID
MONITOR
MAINTAIN
A safety analogy

If you want to reduce driving risk:
Learn the rules
  • Read / Take a course
Learn how to drive safely
  • Get qualified instruction
  • Develop safe driving habits
Take protective measures
  • Don’t drive recklessly
  • Wear seatbelts
Get a safer car
  • Perform regular maintenance

If you want to reduce Internet risk:
Learn the rules
  • Read / Take a course
Learn how to use the web safely
  • Get qualified instruction
  • Develop safe internet use habits
Take protective measures
  • Don’t “surf & click” recklessly,
Buy a safer computer or OS
  • Make your computer/network safe,
  • Perform regular maintenance
Maintenance is required

**Regular maintenance**
- Clean it regularly (wash & polish)
- Change fluids (oil, coolant, etc.)
- Check for wear (brakes, tires, etc.)
- Replace worn parts (tires, brakes, etc.)

**Regular maintenance**
- Clean it regularly (clear cache, etc)
- Update software & virus definitions
- Monitor credit and financial accounts
- Replace outdated hardware and software
One of the ways that bad guys can do damage is by taking advantage of flaws in software. These flaws allow the criminals to make the software do things it normally wouldn’t, and often they’ll give an attacker a way into gaining control over the computer and the files on it.

That’s why it’s so important to update the software or apps that you use as soon as the updates are available. You wouldn’t let a leaky gas tank keep dripping, would you?
Software Updaters

Portable Apps
Portable SUMo
Portable Software Updater

Installed Apps
OUTDATEFighter
Kaspersky Software Updater
FileHippo

Microsoft Patch Tuesday
Keep your system “clean”

CCleaner, is a widely popular and free tool from Piriform software, there is also Mac OS version.

It improves system security by clearing cookies and other potentially security compromising files from the browser cache. It also improves system performance by cleaning up temporary files left by numerous applications and by correcting errors and optimizing the registry.
Now for the Bad News

• Unless your computer is only a few months old, your antivirus software is outdated and may not be able to detect the newest, polymorphic viruses.

• Your antivirus software has two distinct parts:
  • A computer program that scans your computer for viruses.
  • Antivirus definitions that tell that program exactly what to look for.

• Updating your antivirus definitions—which you should do frequently—is **not** the same thing as updating your antivirus software.
Out with the old, in with the new.

Just like you need to change the oil in your car every few months, you need to change your antivirus software every 12 to 18 months.

- Completely uninstall the old version (like that version of Norton Antivirus 2010 you have been using since 2010.)
- Purchase and install the latest version of one of the top rated security suites.
Top rated antivirus software programs

- Bitdefender
- McAfee
- Webroot
- Kaspersky Lab
- Norton by Symantec
Best Free Antivirus Programs

- Avast
- AVG
- Kaspersky Lab
- Bitdefender
Back It Up

So much of our lives are on our computers and phones now, from precious photos and videos of loved ones to crucial files and finances for work. For almost all of us, it would be devastating if suddenly we couldn’t access these files, or if these files were lost completely.

The easy solution here is to make sure you keep backups of your files, either via a dedicated cloud backup service on a cloud storage device (e.g. iCloud or Dropbox) or on an external hard drive that you own (e.g. TimeMachine). Better yet, on a mixture of all three!
Implement a backup strategy

Accounts and login credentials
Family photos (digital, of course)
Music library
Videos (personal and commercial)
Documents and Spreadsheets
Email, browser bookmarks, and everything else!
And, don’t forget the value of your time spent trying to recover from a loss

When the inevitable day comes that your hard drive crashes, your data will be gone if you haven’t prepared

Backup is your most important protection

A 4TB drive, dedicated to backups costs less than $100
Back It Up

The key thing is that you backup your files somewhere off the device where those files normally live, so if something happens to that device – you lose it, it breaks, or it gets infected with ransomware – copies of your files are still safe and sound elsewhere.

Don’t keep your local backup device connected to your computer. A ransomware attack will also encrypt all connected devices.

✓ Connect
✓ Backup
✓ Disconnect
Remember…
The Cloud is just someone else’s computer
Use encryption

Data encryption allows us to protect data even when we cannot control who has access to it. High security = good algorithm + strong key (longer = stronger).

You can encrypt data for communication and for storage. You can encrypt an entire storage device, a folder, or a single file.

Unlike simple password protection, which can be cracked, if you forget an encryption key, you cannot retrieve the data without a brute force attack.
Encrypting communication

To protect your log-in credentials when using wireless networks, public networks, or public computers. Used by banking and most shopping websites, but less often by others.
You should also use it for your e-mail and Social Networking, especially when you are not on a safe network.
Cannot protect against keyloggers!
Encrypting stored data

You can encrypt an entire storage device, a folder, or a single file.

Full drive encryption is good, but has some drawbacks.

MacOS comes with FileVault

Windows 10 Professional comes with BitLocker

You can purchase encryptable external storage devices
Encryption Tools
People and passwords

Basic problems with people and passwords/encryption keys:
Long passwords and keys with random characters are often too hard to remember.
We don’t like typing long, complex passwords or keys.
We cannot remember more than a few passwords/keys, so we reuse the same ones over and over.
All reasons to use a Password Manager
Password Generators

1Password - Password Generator

Password Length: 24

- Allow digits
- Allow symbols
- Allow ambiguous characters
The worst password is the one you forget.
Use Multi-factor Authentication

Use multi-factor authentication when ever possible

Multi-factor authentication (MFA) is a method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories:

• Knowledge (something they know)
• Possession (something they have)
• Inherence (something they are).

Multi-factor Authentication
Select a browser and security add-ons

Both of these browsers are:

- OS dependant
- Have add-ons with top notch security
- Open source
- Free
- Large user base
- Very large number of add-ons
VPN stands for Virtual Private Network, it is a technology that creates a secure network connection over the unsecure Internet. All traffic over a VPN is encrypted to secure data integrity, privacy and prevent any unintentional interception of data.

A VPN will help defend against mass surveillance by governments, corporations or hackers. It will keep your real IP address and location private and your Internet Service Provider (ISP) or public WiFi-hotspot cannot decipher your internet traffic or know which websites you have visited.
VPN Services

NordVPN
ExpressVPN
VyprVPN
ZenMate
F-Secure
Windscribe
Lock down your home network

Secure your local network, your computers, and your smartphones

Start with your router:

• Change the log-in credentials from the default
• Ensure you set a strong password
• If you have wireless, enable encryption with a strong encryption key and turn off ID broadcasting
• Use an alternative DNS provider
• Ensure the NAT firewall is enabled
• Update the firmware
Perform scheduled system maintenance

Daily
- Update anti-virus definitions

Weekly
- Run virus scan
- System backup
- Data backup
- Apply software maintenance
- Clean system

Monthly
- Take a copy of backups to an off-site location
Perform scheduled account and credit monitoring

Daily
- Save charge and debit card receipts

Weekly, bi-weekly, or monthly
- Compare debit and credit purchases to on-line records
- Note discrepancies and address

Clean system
- Three times a year

Obtain free copy of credit report and examine for mistakes and new accounts you did not open
Identity Theft Protection

There are a number of identity theft protection services with varying cost structures. You might seriously consider signing up for one. I know from personal experience the up-front cost is well worth the services provided when you need them.
Portable Apps

Portable apps might better be described as portable software.

- It is software that does not require installation to the computer, you run the software from a flash drive.
- Settings and configuration are with the software and not the PC.
- It leaves no (or virtually no) footprint on the computer (no registry keys or temporary files).
- There are apps for both Windows and a limited number for Mac OS systems.
- Best of all, it is open source most apps are free.
This presentation was created following the Fair Use Guidelines for Educational Multimedia. Certain materials are included under the Fair Use exemption of the U.S. Copyright Law. Further use of these materials and this presentation falls under the following terms.

Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)