Computer Security and Safety Information

Summary

The following article contains information on computer and network security from malware, spyware, viruses and phishing schemes. Following these recommendations will not keep you 100% safe, but it will reduce potentially unwanted risks to your personal data and your computer.

Passwords

Passwords are your first line of defense when it comes to computer and network security. Do not share your password with anyone. Do not write your password down in a place easily accessible to others. If you believe your password has been compromised, change your password immediately.

Importantly, do not reuse your passwords! Data breaches will definitely happen. If you have a unique password for every site, service or device that requires one any data breach will likely not have far reaching consequences for you. If that seems daunting, trying using a password management program. We recommend 1Password.

Password length is important along with including numbers and symbols for added complexity. For important services, a password of at least 12 characters, but ideally 15 is currently recommended (as of 2019). Decryption programs continue to get better and better with time, requiring a longer and longer password for added protection. A good countermeasure is to enable multi-factor authentication on any site, service, or app that offers it. The tenant of multi-factor is it combines something you know (your password) with something you have (like your cell phone for example).

Be Vigilant...Don't Just Click!

The first rule of computer security can be summed up with this statement, **don't just click**. Internet scams are incredibly prevalent and the best way to protect yourself is to never click a link in an email, social networking message or reply to an email/message requesting personal information. This includes account numbers, account names (usernames), passwords, ID numbers, Social Security numbers, date of birth or anything you would consider personal information. A majority of emails requesting personal information are known as Phishing emails. They appear to be from a trusted and established organization; in reality they are an attempt to gain access to your account or steal information. This also applies to websites; be wary of free offers and contests. Do not click or reply if you are unsure of its source or why you got it!

If you ever have a question about an email you received (to your Bethel email address) please contact the ITS Help Desk for more information or verification of authenticity.

Verify "Auto Update" is On

Mac OS

The Mac OS software update program will automatically check for new updates on weekly basis for you to download and install. In Mac OS 10.5 (and later) you can enable the OS to automatically download and install high priority updates to your computer. The following link provides you with additional information about the Mac OS software update utility.

Windows

Check frequently for updates using Windows Update in the Settings app on your windows PC: Settings Windows Update

Windows Update will download updates automatically but won't always install them until you restart your computer.

Use Anti-Virus Software

Anti-virus software does not guarantee that your computer will not become infected, but it will limit infections. If you do not have anti-virus software please consider one of the following free options.

Windows

If you are looking for free anti-virus software to install the Help Desk suggests using Malwarebytes. It is a free product that works extremely well.

Malwarebytes

Note: *Windows 8 and above users, Windows Defender is automatically on your computer and works great as an Anti-Virus software.*

Avoid Spyware & Malware

Always exercise caution when installing free software. In particular be cautious around Internet pop-ups offering free computer scans. Websites and programs can include spyware or fake pop-ups which will attempt to trick you into doing something. If you believe you have been infected by malware below are some tools you can use for scanning and removing these infections.

Malwarebytes (free and paid version available)

Computer Firewalls

Operating System Firewalls

Both Microsoft Windows and Apple Macintosh OS X contain built-in firewalls. In Windows, this is on by default. In Mac OS X the firewall needs to be manually turned on.

Internet Security Suites and 3rd Party Firewalls

Third-party firewalls, such as those provided by Internet security suites, are very comprehensive, but have been known to cause connection problems when accessing secure Bethel University websites from off-campus. In these situations, resolving the problem will require students to work with the software maker or to disable the software when accessing Bethel University Resources.

VPN Services

Employees at Bethel University have access to our VPN service, Cisco Any Connect. This will enable all internet traffic to be routed through our campus security appliances for your protection. Its required for off-campus access to our secure file storage network and recommended for use on any network that you do not otherwise trust (i.e., the free wifi at your local coffee house of choice). Its also the ideal way to safely browse the internet while abroad and will pull an IP address from our network, effectively "masking" your devices as being in the U.S.

For students, the Help Desk recommends using a paid-for service. There are many VPN services out there and our current suggestion is NordVPN. You may experience slower web browsing while using a VPN.