Safe Browsing

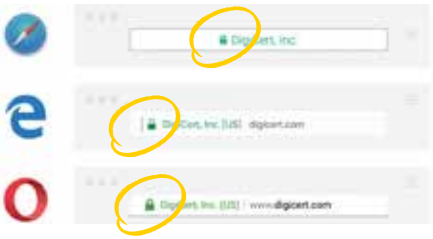
Avoid sharks while surfing online

The Internet can be a risky place. There are plenty of crooks online looking to scam you, lots of websites that look safe but steal your information, and many applications that contain malware that will infect your device. Google estimates that 56 percent of global email is spam, 40 percent web sites are fake, and 21 percent of apps for phones are malicious. The 4th theme area of the Cybersecurity Awareness Campaign is about how to protect yourself online.

> A key to keeping information secure is to encrypt it so that others cannot read it.

Look for the lock

When browsing the web, your web browser will provide indication if the website that you are browsing to is secure. This is shown by locks or a notification in the address bar like this:



It is becoming standard practice for all reputable sites to use secure connections all the time. All the major social networks (Facebook, Snapchat, etc), shopping sites (Amazon, eBay), search engines (Google, Bing), and news (CBC, Huffington Post, CNN) use secure connections. If you don't see the lock or your browser tells you the page is "Not secure" then you should think twice about using that website.

Encrypt and use VPN

A key to keeping information secure is to encrypt it so that others cannot read it. You can do this by using BitLocker on Windows or FileVault2 on Macs. You can also use a Virtual Private Network (VPN) when using the Internet to make sure people cannot intercept your traffic.

The University provides a free VPN called GlobalProtect. You can find out how to install it at **uwindsor.ca/vpn**

Patch and reboot regularly

Computers and devices run using computer programs that operate the hardware (operating system) and enable access to services and functionality (software). These computer programs are not perfect, and they contain errors (bugs) that can provide a means for a hacker to gain access to your device or data. These bugs are corrected by software updates, patches and fixes.

You should:

- Apply operating system updates
- Install software (like web browser) updates
- Accept mobile app updates
- Enable automatic updates
- Reboot your device regularly

Generally all you need to do is reboot your device and it will update as it restarts.

Wear your seatbelt

Antivirus is the oldest trick in the book. It's like putting on your seatbelt when you get in the car. It should be mandatory and automatic.

Antivirus is software used to defend a computer against viruses, trojans and other malicious software. It is essential on Windows PCs and encouraged for Macs, Linux and mobile devices.

The University installs anti-virus on all office PCs and provides free anti-virus from Sophos to all faculty, staff and students for their home machines. Find installation instructions here: **uwindsor.ca/antivirus**

SOPHOS

cybersecurity awareness
UNIVERSITY OF WINDSOR

We're here to help!

IT Services is happy to answer questions about cybersecurity on campus: **ext. 4440** or open a ticket for service here: **uwindsor.ca/itshelp**. More information on cybersecurity issues facing campus: **uwindsor.ca/cybersecurity**