
UNBC
UNIVERSITY OF
NORTHERN BRITISH COLUMBIA
S.A.F.E Computing

STUDENT

Contents

S.AF.E Computing

Safe Browsing

Common mistakes that everyone makes

- Many users have a tendency to click on links without considering the risks of their actions.
- Web page addresses can be disguised or take you to an unexpected site.
- Many web browsers are configured to provide increased functionality at the cost of decreased security.
- New security vulnerabilities may have been discovered since the software was configured.
- Computer systems and software packages may be bundled with additional software, which increases the number of vulnerabilities that may be attacked.
- Third-party software may not have a mechanism for receiving security updates.
- Many websites require that users enable certain features or install more software, putting the computer at additional risk.
- Many users may not know how to configure their web browsers securely.

As a result, exploiting vulnerabilities in web browsers has become a popular way for attackers to compromise computer systems.

Tips for safe browsing:

- **Keep your browser software up-to-date:** This is crucial, as new patches are often released to fix existing vulnerabilities in browser software. This recommendation doesn't apply solely to browser software – it is critical to keep operating system software and any other software you have up-to-date for the same reason.

- **Run anti-virus software:** Anti-virus software provides protection by scanning for and removing malicious files on your computer. There are many excellent options for virus protection software (both paid and free), so it is up to you to do a little research and select a program that best fits your needs.

- **Scan files before downloading:** It is important to avoid downloading anything until you're confident that it is secure. If you have any suspicion that a file may not be legitimate or may be infected, scan it with antivirus software before downloading.

- **Watch out for phishing:** Phishing attacks use online communications (usually email) to trick users into giving out their sensitive information. Often times these messages appear to be from banks, social media sites, shopping sites, or payment processers. Phishing messages frequently contain links that lead to counterfeit versions of popular sites. You can avoid falling victim to phishing schemes by ignoring unsolicited messages and not clicking on hyperlinks or attachments in emails (type or copy/paste the URL as it appears instead).

- **Don't reuse passwords:** Using the same password for multiple sites only makes it easier for attackers to compromise your sensitive information. Instead, use a program like KeePass or 1Password to keep track of your passwords.

- **Use HTTPS:** The "s" in "https" stands for secure, meaning that the website is employing SSL encryption. Check for an "https:" or a padlock icon in your browser's URL bar to verify that a site is secure before entering any personal information.

- **Read privacy policies:** Websites' privacy policies and user agreements should provide details as to how your information is being collected and protected as well as how that site tracks your online activity. Websites that don't provide this information in their policies should generally be avoided.

- **Regularly monitor your bank statements:** Keeping an eye on your online statements will allow you to react quickly in the event that your account has been compromised.

- **Be careful using public or free Wi-Fi:** Attackers often use wireless sniffers to steal users' information as it is sent over unprotected networks. The best way to protect yourself from this is to use UNBC's VPN client (https://vpn.unbc.ca).

- **Disable stored passwords:** Nearly all browsers and many websites in general offer to remember your passwords for future use. Enabling this feature stores your passwords in one location on your computer, making them easier for an attacker to discover if your system gets compromised. If you have this feature enabled, disable it and clear your stored passwords.

- **Turn on your browser's popup blocker:** Popup blocking is now a standard browser feature and should be enabled any time you are surfing the web. If it must be disabled for a specific program, turn it back on as soon as that activity is complete.

- **Use your browser's Private Mode**

For Chrome: https:\\support.google.com\chrome\answer\95464?hl=en

For Firefox: https:\\support.mozilla.org\en-us\kb\private-browsing-use-firefox-without-history

For Ipad, Iphone: https:\\support.apple.com\en-ca\HT203036

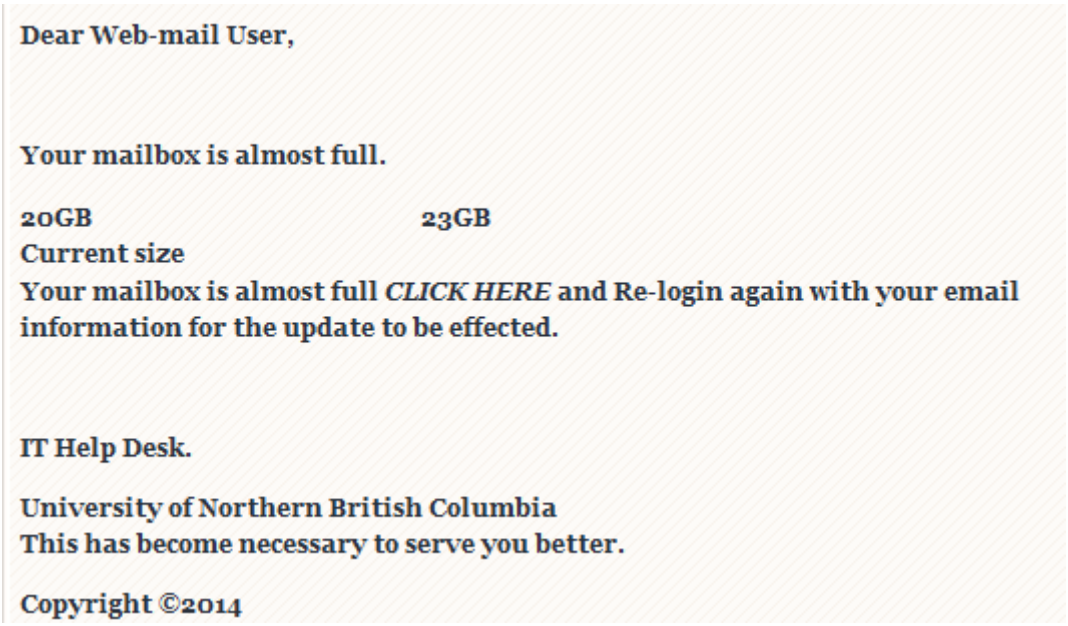
For Safari: https:\\support.apple.com\kb\PH19216

S.A.F.E Computing

Phishing

Spot the Phishing Email

1.



Dear Web-mail User,

Your mailbox is almost full.

20GB **23GB**
Current size
Your mailbox is almost full *CLICK HERE* and Re-login again with your email information for the update to be effected.

IT Help Desk.

University of Northern British Columbia
This has become necessary to serve you better.

Copyright ©2014

2. Hello Sally,

Due to recent spam and phishing exploits, we need to confirm that your account has not been compromised.
Please click the link below to visit the UNBC website and verify that your account is safe.

http://www.unbc.ca/its/confirm.php

If you have any questions or concerns, please reply to this message.

Thank you.

Account Management Team
Information Technology Services

University of Northern British Columbia
3333 University Way
Prince George, BC

V2N 4Z9

3. Please be advised to uprade your E-mail account, we will be performing system wide maintence. during this maintence all user are advised to login with the below link

https://docs.google.com/spreadsheet/viewform?formkey=dEwyT1hKamxMSndrb1B1MTJTdWxzekE6MQ

To help expend there UNBC account limit, login with your User name and Password and click on Submit button.

THis message is from UNBC Web Admin

If you said all three you were correct. Here's some tips on how to spot a phishing email.

Urgent action required. Fraudsters often include urgent "calls to action" to try to get you to react immediately. Be wary of emails containing phrases like "your account will be closed," "your account has been compromised," or "urgent action required." The fraudster is taking advantage of your concern to trick you into providing confidential information.

Generic greeting. Fraudsters often send thousands of phishing emails at one time. They may have your email address, but they seldom have your name. Be skeptical of an email sent with a generic greeting such as "Dear Customer" or "Dear Member".

Link to a fake web site. To trick you into disclosing your user name and password, fraudsters often include a link to a fake web site that looks like (sometimes exactly like) the sign-in page of a legitimate web site. Just because a site includes a company's logo or looks like the real page doesn't mean it is! Logos and the appearance of legitimate web sites are easy to copy. In the email, look out for:

Links containing an official company name, but in the wrong location. (for example www.unbc.com)

Legitimate links mixed with fake links. Fraudsters sometimes include authentic links in their spoof pages, such as to the genuine privacy policy and terms of service pages for the site they're mimicking.

These authentic links are mixed in with links to a fake phishing web site in order to make the spoof site appear more realistic.

Look for these other indicators that an email might not be trustworthy:

- Spelling errors, poor grammar, or inferior graphics.
- Requests for personal information such as your password, Social Security number, or bank account or credit card number. Legitimate companies will never ask you to verify or provide confidential information in an unsolicited email.

Attachments (which might contain viruses or keystroke loggers, which record what you type).

S.A.F.E Computing

Malware & Viruses

"Malware" is short for malicious software and used as a single term to refer to virus, spy ware, worm etc. Malware is designed to cause damage to a stand alone computer or a networked pc. So wherever a malware term is used it means a program which is designed to damage your computer it may be a virus, worm or Trojan.

Virus: Virus is a program written to enter to your computer and damage/alter your files/data. A virus might corrupt or delete data on your computer. Viruses can also replicate themselves. A computer Virus is more dangerous than a computer worm as it makes changes or deletes your files while worms only replicates itself with out making changes to your files/data.

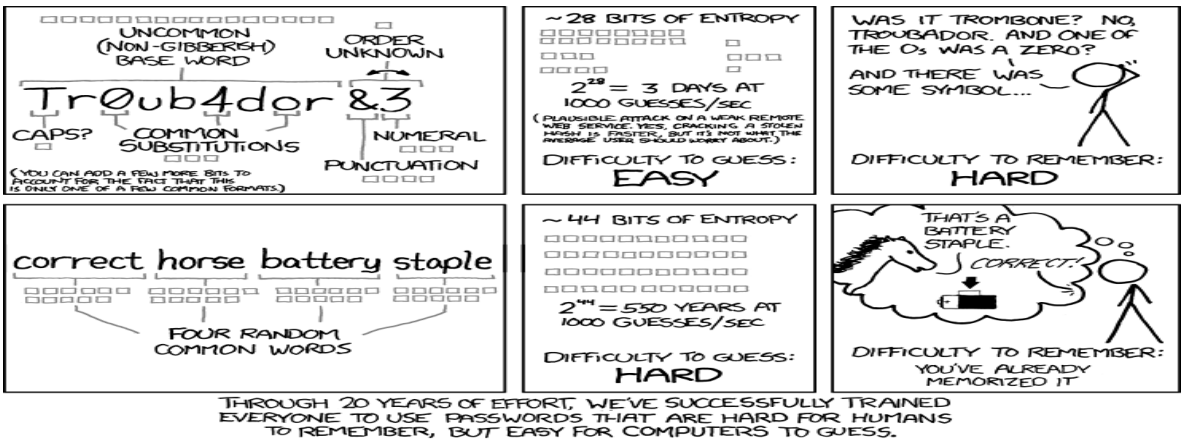
Trojans: - A Trojan horse is not a virus. It is a destructive program that looks like a genuine application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. Trojans also open a backdoor entry to your computer which gives malicious users/programs access to your system, allowing confidential and personal information to be theft.

Adware: - Generically adware is a software application in which advertising banners are displayed while any program is running. Adware can automatically get downloaded to your system while browsing any website and can be viewed through pop-up windows or through a bar that appears on a computer screen automatically. Adwares are used by companies for marketing purpose.

Spyware: - Spyware is a type of program that is installed with or without your permission on your personal computers to collect information about users, their computer or browsing habits tracks each and everything that you do without your knowledge and send it to remote user. It also can download other malicious programs from internet and install it on the computer. Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware type program or application.

Spam: - Spamming is a method of flooding the Internet with copies of the same message. Most spams are commercial advertisements which are sent as an unwanted email to users. Spams are also known as Electronic junk mails or junk newsgroup postings. These spam mails are very annoying as it keeps coming every day and keeps your mailbox full.

Ransomware: Ransomware is an advanced type of malware that restricts access to the computer system until the user pays a fee. Your screen might show a pop up warning that your have been locked out of your computer and that you can access only after paying the cyber criminal. The cyber criminal demands a ransom to be paid in order for the restriction to be removed. The infamous Cryptolocker is one type of ransomware.



How to avoid malware (from https://antivirus.comodo.com)

1. Beware of being tricked into downloading malware.

2. Beware of messages from unknown sources that instruct you to download software, especially if it says that it is to protect you.

3. Beware of clicking on banner ads.

4. Install antivirus and antispyware programs from a trusted source

5. Update software regularly. Subscribe to automatic software updates

6. Uninstall software that you don't use.

7. Use strong passwords. Strong passwords are at least 10 characters long and include a combination of letters, number special characters

8. Never turn off your firewall.

9. Be careful when using flash drives. Don't put an unknown stick into your PC.

10. Don't open unknown email. Hackers send out millions of spam emails looking for a few unwitting victims.

11. When installing software, be careful not to select bundled tool bars and add-ons. These frequently create performance problems and are often malicious

12. Never leave a list of password and ids around where people can find it. No post it notes!

13. Do not base your passwords on personal information that could be guessed. That would include your name, your close relative's names, your date of birth, etc.

What makes a strong password?

A strong password will adhere to the following rules:

1. Contain 10 or more characters.
2. Include Alpha, numeric and special characters (&,!, etc.).
3. Include a mix of upper and lower case letters.
4. Never use a sequence of number (1234).
5. Does not duplicate your user id in the password.

Passphrases vs passwords:

While passwords and passphrases essentially serve the same purpose – providing access to secure services or sensitive information – passwords are generally short, hard to remember and easier to crack. Passphrases are easier to remember and type. They are considered more secure due to the overall length of the passphrase and the fact that it shouldn't need to be written down. Here are some tips for creating a good passphrase:

- Make up a sentence or a phrase that includes a combination of upper and lower case letters, special characters and punctuation.
- * Include some memorable "encoding" in the phrase.

For example, "PG winters are cold" would be an acceptable passphrase, as it meets the 10 character requirements. If you wanted to add a bit of complexity to your passphrase, consider "Pg w1nters are c0ld!".

S.A.F.E Computing

Protecting your mobile devices

Keep Your Smartphone/Tablet Safe

- Never leave your smartphone or tablet unattended in a public place or office.
- Do not leave your device unsecured in a hotel room when you go out – instead lock it in the safe.
- Do not get distracted by strangers in a public place when your phone is on a table or in an open handbag or briefcase.
- If keeping your device with you when out and about, ensure it cannot be accessed by pickpockets.
- Keep your home or office secure against burglars and illicit callers.
- Do not leave smartphones and tablets on view through windows and glass doors.
- Never leave smartphones or tablets visible in a car. Even if you are in the car, your laptop could be vulnerable to theft when you are stationary (for example, whilst parking or at traffic lights).
- Always password-protect access to your smartphone or tablet.
- Fingerprint recognition offers a degree of safety, but there is still no substitute for a well-devised and protected password or PIN.
- Be careful how you dispose of packaging that might advertise that you have a new smartphone or tablet.
- Be careful that your smartphone is not easily going to fall out of your back pocket.
- Be wary about damaging your smartphone when in your back pocket, by sitting on it.

Using WiFi

The main security risk associated with using your device in a public place, is that the WiFi may not be secured, enabling unauthorized people to intercept anything you are doing online. This could include capturing your passwords and reading private emails. This can happen if the connection between your device and the WiFi is not encrypted, or if someone creates a spoof hotspot which fools you into thinking that it is the legitimate one.

With an encrypted connection, you will be required to enter a 'key', which may look something like: 1A648C9FE2.

Alternatively, you may simply be prompted to log in to enable internet access. This will tell the operator that you are online in their café, hotel or pub. There is almost certainly no security through encryption.

- Unless you are using a secure web page, do not send or receive private information when using public WiFi.
- Wherever possible, use well-known, commercial hotspot providers .
- Members of the UNBC community wishing to access their network files should use a secure, encrypted Virtual Private Network (VPN).

Bluetooth

- Ensure that your Bluetooth is switched off when you do not need to use it.
- If you do use Bluetooth, make sure that your devices are not left ‘discoverable’.
- Do not pair devices in public in case someone is scanning you while you create the connection.
- If possible, restrict access to known, paired devices.
- Do not accept files transmitted via Bluetooth from unknown or suspicious sources.

S.A.F.E Computing

Theft Prevention

10 Tips to Safeguard your Assets

1. **Keep your personal information safe.** An identity thief will pick through your garbage or recycling, so be sure to shred receipts, copies of credit applications, insurance forms, etc.

2. **Keep personal information confidential.** Do not give out personal information on the phone, through email or the Internet unless you initiated the contact and know who you're dealing with.

3. **Be aware of billing and statement cycles.** If your bills or statements don't arrive on time, follow up immediately to ensure they have not been fraudulently redirected. Request electronic statements.

4. **Protect your mail.** Bring in your mail daily. Forward or re-route it if you move, change your mailing address or are away.

5. **Protect your PIN and passwords.** Do not reveal your PIN or passwords to anyone, including employees of RBC, family and friends. When conducting a transaction, keep your card within sight and shield the keypad when entering your PIN.

6. **Limit your risk.** Sign all credit cards as soon as you receive them. If they are lost or stolen, report it immediately.

7. **Unusual transactions.** Beware of "too good to be true" or unexpected offers or requests such as, "You've inherited a large sum of money. To claim it, send us a deposit first." Never agree to conduct financial transactions on behalf of strangers.

8. **Review your transactions.** Regularly review your financial statements to ensure that all transactions are authorized, and report any missing or fraudulent ones. Review your credit bureau file annually.

9. **Limit your exposure.** Only carry credit cards you use. Don't carry your birth certificate and social insurance card when you don't need them, instead keep them in a safe place.

10. **Contact the authorities.** If you suspect you are a victim of fraud or theft, contact the authorities immediately.

S.A.F.E Computing

Email Security

Here are a few tips on keeping your email safe. (from https://antivirus.comodo.com)

1. Don't open attachments unless you are sure you know who it is from. Merely have a known sender email is not enough because spam spoofing.
2. Don't fall for "security notices" supposedly sent by financial institutions or your "email administrator". These are almost always scammers attempting to trick you into disclosing your login credentials.
3. Do not follow web links you receive via email. If you are tempted, you can right click on the link and view the real link address as opposed to the text that display. If they do not match, it is a trap.
4. Use multiple email addresses and do not give out the address you use most for personal communication to anyone except known contact.
5. Change your password regularly and keep it in a safe place.
6. Use a strong password, consisting of at least 8 characters including combinations of upper and lower case, alpha and numeric plus one special character.
7. Keep your personal information personal – don't share bank or credit card information by email.
8. 8. Make sure that you have antivirus software installed and keep it up to date.
9. Use digital email certificates to secure your communication and prevent message tampering.

Using safe email practices helps you:

- **Protect your inbox**
- **Protect your computer**
- **Protect your privacy**
- **Protect your friends and neighbors**

Here are recommendations you should follow to protect yourself when using email.

1**. Screen messages before viewing them, and delete anything that appears suspicious.**

· Carefully examine your list of unopened messages**.** Do any of them come from people or addresses you don't recognize? Do the subject lines have words with too many spaces, or long random numbers? Do they seem too good to be true, or somehow odd? If so, it's probably best to just delete the message along with any attachments.

· **Wait! Don't open that email yet...** If a message has attachments don't open it unless you know the sender and are expecting the attachment. If you're not sure what it is, contact the sender before opening the message and ask exactly what the message and attachment is.

2. Don't be fooled by Dirty Tricks. Most computer worms (a kind of malicious program) spread themselves via email by spoofing addresses found in the infected computer's address book and sending copies of itself to other addresses in the address book, so it's very likely that an infected message can appear to come from someone you know. Many of these messages will use vague or generic subject lines like "Re: " or "Hi." Others will try to look like they come from a technical support service, or even from Microsoft. Be careful about opening these.

3. **Open your messages, but beware the Next and Previous buttons.**

Using the Next and Previous buttons to open and move from message to message is convenient but dangerous, especially if you don't screen messages thoroughly, or if new messages come in while you're reading other screened messages.

4. **Handle Attachments Safely.**

· **Don't open attachments unless you are absolutely sure about what they are and who they came from.** Even attachments that were sent directly to you by a known sender might contain malicious code.

· **Be especially careful with MS Word & Excel files.** When opening Microsoft Word or Excel attachments containing macros, always select the "Disable Macros" option if you are not sure if there should be a macro.

· **Beware of Dangerous File Types!** Some file types have been deemed unsafe by Microsoft. Most of these file types are executable or exploitable and are considered unsafe to send and receive as email attachments. SSU's email servers scan all incoming email messages for attachments using these unsafe file types. If you also use an off-campus email address, you should be aware of these unsafe file types.

· **Windows Users - Make Extensions Visible** Some malicious attachments will "pose" as a harmless file type like digital image by including that file type extension in it's name. You might get an attachment called "hawaii.jpg" and think it's a picture from your friend's vacation. But it might actually be a .pif file, one of the exploitable file types. This can happen because Windows does not display file extensions by default, so a .pif file named"hawaii.jpg.pif" will appear as "hawaii.jpg"

5. Don't Unsubscribe.

Spammers often include an "unsubscribe from this list" link in their messages. This makes them appear more responsible and reputable, but they often use this as a way to confirm your email address so they can send you more spam or sell your email address to other spammers. If you don't want it, mark it as junk and delete it.

6. Be a Good Internet Citizen.

- Don't use your email in ways that will contribute to the problem.
- Don't send unsolicited email and attachments.
- Don't forward chain letters.
- Don't respond to or participate in email hoaxes.
- Don't send attachments which use the "unsafe" file types.
- Don't post your UNBC email address (or other student's addresses) on publicly accessible web pages.
- Use a "disposable" email account (a free account from gmail or hotmail) for online shopping and posting to off-campus online discussion boards.

S.A.F.E Computing

Copyright

People occasionally confuse copyright with patents, trademarks, industrial designs and integrated circuit topographies. Although all of these are forms of intellectual property, they differ as follows:

- **Copyright** provides protection for literary, artistic, dramatic or musical works (including computer programs) and other subject-matter known as performer's performances, sound recordings and communication signals.
- **Patents** cover new inventions (process, machine, manufacture, composition of matter) or any new and useful improvement to an existing invention.
- **Trademarks** may be one or a combination of words, sounds or designs used to distinguish the goods or services of one person or organization from those of others in the marketplace.

What is protected by copyright?

Copyright applies to all original literary, dramatic, musical and artistic works provided the conditions set out in the *Copyright Act* have been met. Each of these general categories covers a wide range of creations, including:

- **literary works**: books, pamphlets, computer programs and other works consisting of text;
- **dramatic works**: motion picture films, plays, screenplays, scripts, etc.;
- **musical works**: musical compositions with or without words; and
- **artistic works**: paintings, drawings, maps, photographs, sculptures, plans, etc.

Copyright also applies to subject-matter other than works, consisting of:

- **performer's performances** meaning any of the following when done by a performer:
- a performance of an artistic, dramatic or musical work, whether or not the work was previously fixed (recorded) and whether or not the work's term of copyright protection has expired;
- a recitation or reading of a literary work, whether or not the work's term of copyright protection has expired; and
- an improvisation of a dramatic, musical or literary work, whether or not the improvised work is based on a pre-existing work.
- **sound recordings**: recordings consisting of sounds, whether or not a performance of a work, but excludes any soundtrack of a cinematographic work where it accompanies the cinematographic work

The Fair Dealing Exemption

The fair dealing exemption in the *Copyright Act* (sections 29, 29.1 and 29.2) provides that fair dealing with a copyright-protected work for one of the following eight purposes: research, private study, criticism, review, news reporting, education, satire or parody, does not infringe copyright. Any fair dealing for the purpose of news reporting, criticism or review must however mention the source and, if given in the source, the name of the author or creator of the work.

Depending on the circumstances, a student may copy or communicate an extract of a copyright-protected work under the fair dealing exemption without the permission of the copyright holder and without infringing copyright, provided that they only copy a **short excerpt** of the work.

Students should also remember to correctly credit their source when using short excerpts, not just for the purpose of criticism or review.

The Fair Dealing Policy defines a short excerpt as follows:

> A short excerpt includes:
>
> > (a) up to 10% of a copyright-protected work (including a literary work, musical score, sound recording, and an audiovisual work)
> >
> > (b) one chapter from a book
> >
> > (c) a single article from a periodical
> >
> > (d) an entire artistic work (including a painting, print, photograph, diagram, drawing, map, chart, and plan) from a copyright-protected work containing other artistic works
> >
> > (e) an entire newspaper article or page
> >
> > (f) an entire single poem or musical score from a copyright-protected work containing other poems or musical scores
> >
> > (g) an entire entry from an encyclopedia, annotated bibliography, dictionary or similar reference work
> >
> > provided that in each case, no more of the work is copied than is required in order to achieve the allowable purpose.

For questions about copyright or help with citations, please contact Patrice Hall in the Geoffrey C. Weller Library (Patrice.Hall@unbc.ca)

S.A.F.E Computing

Social Networking

- Use strong passwords.

- Keep your profile closed and allow only your friends to view your profile.

- What goes online stays online. Do not say anything or publish pictures that might later cause you or someone else embarrassment.

- Never post comments that are abusive or may cause offence to either individuals or groups of society.

- Be aware of what friends post about you, or reply to your posts, particularly about your personal details and activities.

- Remember that many companies routinely view current or prospective employees' social networking pages, so be careful about what you say, what pictures you post and your profile.

- Learn how to use the site properly. Use the privacy features to restrict strangers' access to your profile. Be guarded about who you let join your network.

- Be on your guard against phishing scams, including fake friend requests and posts from individuals or companies inviting you to visit other pages or sites.

- If you do get caught up in a scam, make sure you remove any corresponding likes and app permissions from your account.

- Ensure you have effective and updated antivirus/antispyware software and firewall running before you go online.

What makes a strong password?

A strong password will adhere to the following rules:

1. Contain 10 or more characters.
2. Include Alpha, numeric and special characters (&,!, etc.).
3. Include a mix of upper and lower case letters.
4. Never use a sequence of number (1234).
5. Does not duplicate your user id in the password.

Passphrases vs passwords:

While passwords and passphrases essentially serve the same purpose – providing access to secure services or sensitive information – passwords are generally short, hard to remember and easier to crack. Passphrases are easier to remember and type. They are considered more secure due to the overall length of the passphrase and the fact that it shouldn't need to be written down. Here are some tips for creating a good passphrase:

- Make up a sentence or a phrase that includes a combination of upper and lower case letters, special characters and punctuation.
- * Include some memorable "encoding" in the phrase.

S.A.F.E Computing

Cyberbullying

What is cyberbullying?

- Sending mean and sometimes threatening emails or text messages.
- Spreading gossip, secrets or rumours about another person that will damage that person's reputation.
- Breaking into an email account and sending hurtful materials to others under an assumed identity.
- Creating blogs or websites that have stories, cartoons, pictures or jokes ridiculing others.
- Creating polling websites where visitors are asked to rate individuals' attributes in a negative manner.
- Taking an embarrassing photo of someone with a digital camera and emailing that photo to others.
- Engaging someone in instant messaging, tricking them into revealing personal information and then forwarding that information to others.
- Using someone else's password in order to change their profile to reflect sexual, racist and other content that may offend others.
- Posting false or hurtful messages on online bulletin boards or in chat rooms.

Deliberately excluding others from instant messaging and email contact lists.

Starting in March 2015, another type of cyberbullying has been outlawed. It's illegal to distribute intimate images of a person if you know that they did not consent to that image being distributed—or if you are reckless about whether the person gave their consent to that image being distributed. "Reckless" means you know the person may not have consented to the image being distributed, but you don't care.

Cyberbullying may also be defamation. The *Criminal Code* (section 300) outlaws publishing a defamatory libel – material published, without lawful justification or excuse, likely to injure the reputation of any person by exposing them to hatred, contempt or ridicule, or designed to insult the person. But criminal defamation is rare. More common is civil defamation – communication about a person that tends to hurt their reputation.

Reporting an incident of cyberbullying

If you or someone you know at UNBC is experiencing cyberbullying, immediately contact your campus security office. They will engage UNBC IT Security to assist in their investigation and can also escalate situations to the local policing authorities.

S.A.F.E Computing

Cyberstalking

What is cyberstalking?

Cyberstalking is when someone uses the Internet or other electronic means to harass a person. With the prevalence of social media like Facebook and modern cell phone technology, cyberstalking has become more and more common in recent years.

Some examples of cyberstalking include:

- Sending a constant stream of email or instant messages to you, your friends or your family members.
- Posting inappropriate comments or making false accusations on your social media sites.
- Attempting to gather your personal info like your phone number, address, school that can develop into offline stalking behaviors.

Cyberstalking Prevention Tips

- Don't use your real name or a commonly known nickname. Choose a genderless screen name for social websites where your name will be publicly visible.
- Use a separate email account through a free service not tied to your main personal account that you use for online activity.
- Choose a complicated password using letters and numbers that has no significance.
- Don't share your password… ever.
- Don't publish your real name, personal or contact info.
- Set your privacy options as high as possible.
- Don't have personal conversations in publicly viewable forums.
- Refrain from publicizing your personal plans.

How to Handle Cyberstalking Behaviors

- Ignore unknown communications or friend requests sent to you.
- If threat level is low, send a clear message that their communication is unwanted (acts as a benchmark in case of police investigations or legal proceedings). After that, don't send any other communications.
- Do not delete original messages (soft and hard copies).
- Take screen shots (Snipping Tool in Windows 7) of harassing behaviors.
- Stop using site or service (if possible).

In Canada there is no cyberstalking law; however there are provisions in the Criminal Code for Criminal Harassment http://laws-lois.justice.gc.ca/eng/acts/c-46/FullText.html

264. (1) No person shall, without lawful authority and knowing that another person is harassed or recklessly as to whether the other person is harassed, engage in conduct referred to in subsection

(2) that causes that other person reasonably, in all the circumstances, to fear for their safety or the safety of anyone known to them.

Prohibited conduct

(2) The conduct mentioned in subsection (1) consists of

(*a*) repeatedly following from place to place the other person or anyone known to them;

(*b*) repeatedly communicating with, either directly or indirectly, the other person or anyone known to them;

(*c*) besetting or watching the dwelling-house, or place where the other person, or anyone known to them, resides, works, carries on business or happens to be; or

(*d*) engaging in threatening conduct directed at the other person or any member of their family.

Punishment

(3) Every person who contravenes this section is guilty of

(*a*) an indictable offence and is liable to imprisonment for a term not exceeding ten years; or

(*b*) an offence punishable on summary conviction.

Reporting an incident of cyberstalking

If you or someone you know at UNBC is experiencing cyberstalking, immediately contact your campus security office. They will engage UNBC IT Security to assist in their investigation and can also escalate situations to the local policing authorities.

S.A.F.E Computing

Staying Safe at UNBC

There are no guarantees of personal safety in any environment. It is incumbent upon each individual to safeguard himself or herself against becoming the victim of a crime. One of the best ways to maximize your safety and minimize your risk is to follow some very simple security rules:

- Walk with a friend whenever possible.
- Always be aware of your surroundings and the people around you, no matter whether it is day or night.
- Use well-lighted, well-traveled routes. Avoid dark, vacant or deserted areas.
- Walk with confidence. Show that you are aware and in control. Body language works.
- Trust your instincts. If someone or something makes you feel uneasy, get out or get away.
- If you feel you are being followed, move to a well-lighted and populated area or building, such as a store or restaurant, and call for assistance.
- Know where the emergency telephones are located on campus.

- If you are on campus after hours, stay alert.

- Lock office or lab doors.
- Call Security if you see or hear anything suspicious.
- Tell a friend, colleague or Security where you are and when you plan to leave.
- Arrange to meet a friend or request an escort from Security when you leave.

Offices and Laboratories

- Don't leave your wallet, purse, checkbook, cash or jewelry in open view. Keep them locked away or in a drawer or cabinet.
- Always lock the office or lab door when you leave, even for brief periods of time.
- If you see a suspicious person, or something suspicious, call Security.

Student Residences

- Always lock your door when you leave, even for brief periods of time.
- Secure your belongings, such as lap top computers, back packs, calculators, etc. Do not leave them unattended in a common area such as a hallway, library, lounge, etc.
- Do not allow strangers to enter your room unless they are properly identified. If a stranger does enter your room ask them to leave. If they refuse, create a commotion and leave quickly. Notify Security immediately.
- Don't leave your wallet, purse, checkbook, cash or jewelry in open view. Keep them locked away or in a drawer or cabinet.
- If you see a suspicious person or something suspicious call Security

For information about security initiatives on campus and security tips, please look at http://www.unbc.ca/security

To report an incident to security:

Non-Emergency 250-960-7058

Emergency 250-960-3333

Long Distance 1-866-307-1699

Email security@unbc.ca

S.A.F.E Computing

UNBC Acceptable Use Policy

UNBC Acceptable Use Policy

1.0 Purpose

The purpose of this policy is to promote the responsible and ethical use of the University of

Northern British Columbia (UNBC) computing resources. The computing resources at the

University of Northern British Columbia support the educational, research, and administrative activities of the University. The use of these resources is a privilege that is extended to members of the UNBC community.

2.0 Scope

This policy applies to all users of computing resources owned or managed by the University of Northern British Columbia. Individuals covered by the policy include (but are not limited to) the University of Northern British Columbia faculty and visiting faculty, staff, students, researchers, alumni, guests or agents of the administration, external individuals and organizations accessing network services via UNBC's computing facilities.

Computing resources include:

All university owned, licensed, or managed hardware and software, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

3.0 Acceptable Use Policy

All UNBC computer users are expected to adhere to the computer use policy described here.

In addition, users may be subject to additional regulations set by those responsible for a particular computing facility. Such regulations must be publicized. With due regard for the right of privacy of users and the confidentiality of their data, authorized university staff will routinely monitor computing activity in order to safeguard the security and smooth operation of UNBC computing resources.

Individuals must respect the rights of other authorized users. The following activities are prohibited:

1.

Using the computer access privileges of others or sharing one’s username and password; interfering with the security or confidentiality of other users' files or maliciously destroying any computer stored material including that in primary storage

2.

Impeding others or interfering with their legitimate use of computing facilities (this includes but is not limited to sending obscene, threatening, or repeated unnecessary mail messages or downloading pornographic material);

3.

Illegally copying programs or data that are the property of the university or other users or putting unauthorized or forbidden software, data files, or other such computer-related material on university computers;

4.

Interfering with the normal operation of computing systems or attempting to subvert the restrictions associated with such facilities;

5.

Using computing resources for purposes not in accordance with educational and/or research activity;

6.

Failing to follow specific rules set out by the faculty member or Department in charge of the course for classes, tests, or exams held in a computer lab;

7.

Using the Internet and other computing resources for purposes deemed to be recreational and to the detriment of curriculum-related uses.

4.0

In the event that the University believes a student, employee or guest has violated any part of this policy; the University may suspend or terminate the student’s, employee’s or guest’s computer and/or network access. In addition, violation of this policy may subject students or employees to disciplinary action, up to and including expulsion from the University or termination from employment

Links

UNBC Service Desk

8-265

Support@unbc.ca

1-866-960-5321

1-250-960-5321

UNBC Library

http://www.unbc.ca/library

UNBC Security

http://www.unbc.ca/security

Stay Safe Online

https://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks

https://www.getsafeonline.org

https://texted.ca

Copyright

http://www.cipo.ic.gc.ca/eic/site/cipoInternet-Internetopic.nsf/eng/h_wr02281.html

http://libguides.unbc.ca/copyright

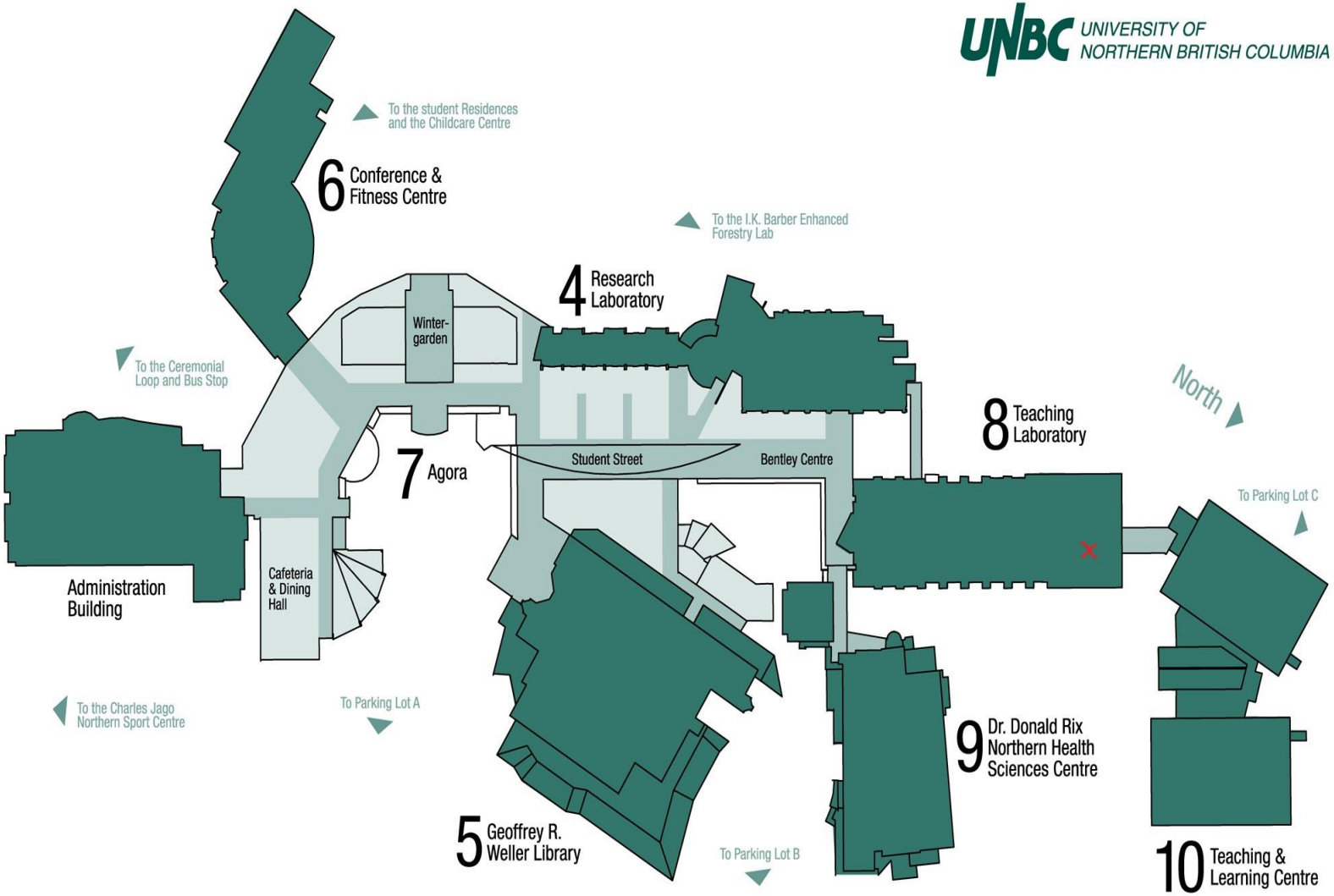
Internet Security

https://antivirus.comodo.com

Criminal Code of Canada

http://laws-lois.justice.gc.ca/eng/acts/c-46/FullText.html

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA



Revised November 2006