Internet Safety: How to Stay Safe Online

Why Internet Safety Matters

- Online threats include malware, phishing, spam, fraud, and scams.
- Protecting yourself online is just as important as physical security.
- Growth in online shopping, banking, and social media increases risks.
- Small actions lead to big protection.

Password Safety

- Use strong, unique passwords.
- Store with a password manager.
- Enable 2-factor authentication (2FA).
- Update regularly and log out on shared devices.

Examples:

- Weak: cat
- Better: SmellyCat!25
- Excellent: $mellyC@t!25
- Other good samples: M0unt_s3ymouR!, B@nana_@venuE?

Browser & Device Security

- Secure browsing: Look for https:// and the lock icon.
- Limit permissions: Only allow mic, camera, or location when needed.
- Block pop-ups and ads: Avoid scareware messages like 'System infected!'.
- Wi-Fi: Don’t use public Wi-Fi for banking. Use a VPN.
- Mobile devices: Keep software up to date, set strong passcodes or biometrics.

Safe Online Shopping

- Shop only on trusted, secure websites.
- Avoid 'too good to be true' deals.
- Use credit cards or PayPal for safer payments.
- Don’t click ads or download buttons on questionable sites.

Social Media Privacy

- Adjust privacy settings (e.g., Facebook’s Privacy Check-Up).
- Limit sharing of personal details.
- Double-check what’s visible to others.

Recognizing Spam & Phishing

Spam: Unwanted promotional emails/messages.
Phishing: Fake emails or texts designed to steal personal info.

Warning Signs:

- Unexpected or suspicious emails.
- Strange sender addresses (support@paypa1.com).
- Urgent language: 'Immediate Action Required!'
- Spelling/grammar mistakes.
- Hidden or suspicious links.

Examples:

- Misspelled, vague email pressuring you for info.
- Familiar logo but urgent tone, pixelated branding, hidden links.
- Fake prize offer with character changes (α instead of a).

Tips:

- Compare with legitimate emails.
- Don’t click unknown links.
- Verify via official websites or phone numbers.
- Mark suspicious messages as Spam/Junk.

Remote Access Scams

- Scammers pose as tech support from trusted companies (Amazon, Microsoft, banks).
- Trick you into installing remote access tools (Anydesk, TeamViewer, LogMeIn).
- Ask for unusual payments (gift cards, Western Union).

Red Flags:

- Pressure to act quickly.
- Aggressive or overly helpful tone.
- Requests for remote access or personal info.

Protect Yourself:

- Never give remote access unless verified.
- Disconnect internet if compromised.
- Uninstall suspicious software, run antivirus.
- Report to your bank and the Canadian Anti-Fraud Centre.

Computer Viruses & Antivirus Protection

- Antivirus prevents malware, spyware, ransomware, phishing attacks.
- Microsoft Defender: built into Windows.
- Paid solutions: offer VPN, identity protection, advanced features.
- Only download software from official stores: Microsoft Store, Apple App Store, Google Play, verified vendor websites.

Final Safety Reminders

- ✓ Use strong passwords
- ✓ Don’t click suspicious links
- ✓ Don’t give out personal info
- ✓ Don’t let strangers access your computer
- ✓ Keep antivirus up to date
- ✓ Be vigilant!

For More Help: Distance Computer Comfort pairs participants with trained tutors across Canada.
Learn more at www.neilsquire.ca/dcc or email mailto:gordonw@neilsquire.ca