Cyber Safety Fundamentals

Blue Sky Net
Jerry Poliszczuk
ICT Community Outreach Coordinator

- Why is cyber security important?
- Understanding the balance between what you can do and what should be left to professional IT services.
- What are common types of attacks?
- Computer security basics.
- Email security - strategies and tactics to avoiding attacks.
- Online safety tips.

Why is Cyber Security Important?

Cyber Safety Fundamentals

Why is cyber security important?

Unfortunately, cyber security is one of those things for a business, organization or individual where you don't really appreciate having it a good system in place until something bad happens.

According to Stats Canada, just over 1 in 5 businesses suffered a cyber security attack in 2017.

The Canadian Chamber of Commerce reported that in 2017, Canadian businesses lost $3 billion due to cyber crime.

Cyber Safety Fundamentals

Why is cyber security important?

Of the 1 in 5 businesses affected by a cyber security attack:

- 39% could not identify the motive of the attack
- 38% identified the motive as an attempt to steal money or demand a ransom payment
- 26% of businesses experienced incidents where perpetrators attempted to access unauthorized or privileged areas.
- 23% faced an incident where there was an attempt to steal personal or financial information.

- 54% of impacted businesses reported that cyber security incidents prevented employees from carrying out day-to-day work.
- 53% reported that incidents prevented the use of resources or services.
- 30% of businesses faced additional repair or recovery costs.
- 10% lost revenue.
- 4% reported that they had to reimburse external parties or make a ransom payment in 2017.

Cyber Safety Fundamentals

Why is cyber security important?

Cyber crime can be extremely costly or disruptive to your business or organization.

So what can you do?

Understanding what you can do when it comes to cyber safety.

Cyber Safety Fundamentals

One of the objectives of this discussion is to help inform you of some of the cyber threats and strategies which you can deploy to protect your business and organization.

From this, it is important to understand which techniques, strategies and practices can be accomplished by yourselves and staff and which are best reserved for your IT professionals.

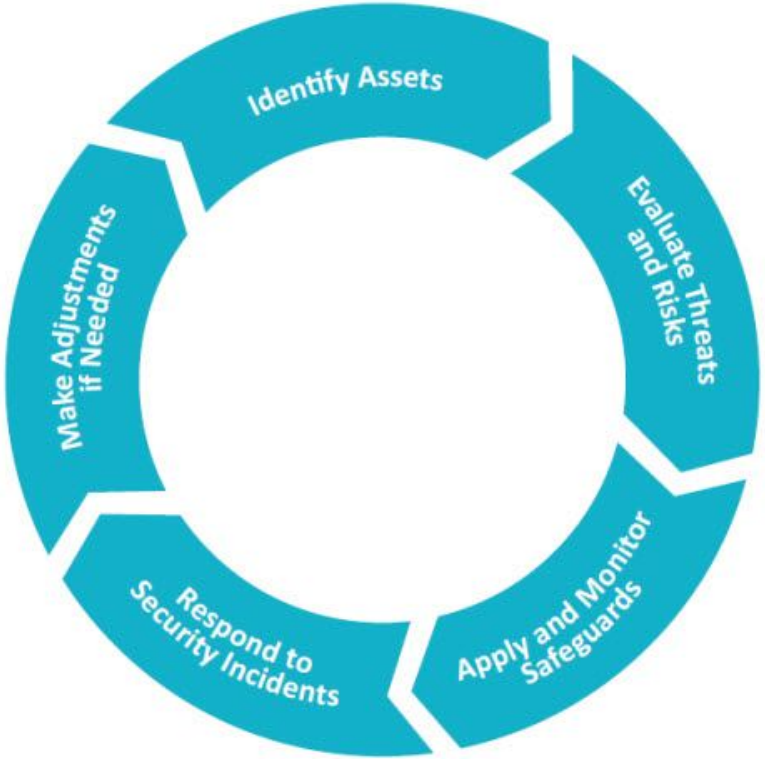
The last thing you'd want to do is cause incidental damage your data, computer or website while performing advanced IT maintenance or IT security tasks!

Cyber Safety Fundamentals

How many people here work somewhere with a IT policy?

Cyber Safety Fundamentals

Your Role in Cyber Safety



https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx#s4

Cyber Safety Fundamentals

IT professionals can assist in formulating a security plan/policy for your business or organization and can assist in the ongoing functions to ensure these are enforced.

Among many other services, IT professionals can assist in developing and implementing security software for your computers, internet networks and help to set in place a data backup procedure.

This helps to not only prevent security threats from being successful, should they be, they mitigate the damage done.

IT professionals can assist in restoring your computers and data in addition to assisting in the removal of malicious software on your computers or websites.

Cyber Safety Fundamentals

Some of the services which IT professionals perform and should be consulted on before doing yourself:

- Help form IT policy to guide staff on best safety practices.
- Secure organizational networks.
- Perform regular updates and backups of your systems.
- Assist in virus removal and restore systems.

Cyber Safety Fundamentals

You will find that many of the techniques employed by those posing cyber threats to be psychological-based, relying on human error to be successful in stealing data or planting viruses.

Ultimately, you are the first line of defense against many cyber security threats and this presentation will assist in providing you with a few tools and insights into what you can do to prevent cyber threats before they cause damage.

IT professionals can further assist in educating staff and implementing best-practices to help prevent threats from being successful attacks.

Cyber Safety Fundamentals

The Golden Rule:

What are common types of attacks?

The psychology behind the common types of technical cyber threats.

Cyber Safety Fundamentals

What are common types of attacks?

Before we discuss topics such as email threats and online safety, it's important to know some of the methodologies which are utilized by perpetrators using tools such as emails and malicious website links.

Having a bit of insight into some of these methods can help prepare you to better identify and scrutinize threats before potentially falling victim to them.

Cyber Safety Fundamentals

What are common types of attacks?

Cyber attacks can come in many forms. Some are designed to bait people into performing certain actions or providing certain information while many others target vulnerable websites or systems.

1. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
2. Man-in-the-middle (MitM) attack
3. **Phishing and spear phishing attacks (Social engineering)**
4. Drive-by attack
5. **Password attack**
6. SQL injection attack
7. Cross-site scripting (XSS) attack
8. Eavesdropping attack
9. Birthday attack
10. Malware attack

Cyber Safety Fundamentals

What are common types of attacks?

In this presentation, we will largely focus on phishing, social engineering and password attacks as these are forms of attacks which you as an individual have the most agency in preventing harmful attacks from being successful and can be seen through a wide range of delivery methods.

Cyber security threats which focus on IT systems such as internet networks or websites should be discussed with your IT department or IT service provider. These threats require more technical preventative measures.

Cyber Safety Fundamentals

Social Engineering Attacks

A social engineering attack is a bit of a broad term as it can be used in varying methods of attacks.

What makes social engineering attacks dangerous is that it relies on human error to be successful, rather than vulnerabilities in software and operating systems. Mistakes made by users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

- Scareware
- Pretexting
- Phishing
- Spear phishing

Cyber Safety Fundamentals

What are common types of attacks?

Scareware

Bombarded with false alarms and fictitious threats. Users are deceived into thinking their system is infected with malware, prompting them to install software which typically end up being malware itself.

Pretexting

A pretexting attack attempts to lure potential victims by crafting a lie and presenting themselves as a trusted institution. In the process, personal information is requested during this process (passwords, social security numbers) - information typically used to confirm identify.

Phishing

Phishing is one of the most popular forms of cyber attacks - typically as email or text messages. They create a sense of urgency or fear which is intended to lessen a person’s ability to calmy review information critically.

Spear phishing

This form of attack is much like a phishing attack, however, it is structured specifically to target a person. The attacker may try tricks such as impersonating a trusted member of staff.

Cyber Safety Fundamentals

What are common types of attacks?

City treasurer was victim of a 'whaling' scam, transferred $100K to phoney supplier

JON WILLING Updated: April 10, 2019

Cyber Safety Fundamentals

Password Attacks

Because passwords are the most commonly used mechanism to authenticate users to an information system, obtaining passwords is a common and effective attack approach.

Access to a person's password can be obtained by looking around the person's desk, they

- Take part in **"sniffing"** the connection to the network to acquire unencrypted passwords
- **Social engineering**
- Gaining **access** to a password database
- Or outright guessing.
    - The last approach can be done in either a random or systematic manner.

Computer security basics.

Cyber Safety Fundamentals

Computer Security Basics.

Ensuring that your business or organization’s computer systems are secured and ready to tackle potential threats is one of the key strategies in preventing cyber threats.

There are some fundamental steps you can take to ensure your systems are secured. Some of these can be done on your own and some may require the help of an IT professional.

- Updating Software
- Anti-virus Software
- Network Security
- Information Backups

Cyber Safety Fundamentals

Updating Software - *Why is it important?*

Software updates are typically provided to help fix issues with your existing software or provide informational updates which help it to perform better.

For example, a software update for your Windows operating system may help fix a potential security issue which Microsoft has identified.

Another example may be your anti-virus software requiring an update as there have been new viruses which have been identified and those virus definitions must be added to your system.

Updating Software - *How do I do it?*

In most cases your software will provide you with a notification which recommends an update to your software.

Software which require updates will typically either prompt you to download and install an update when you open it or will perform the update itself in the background (such as Microsoft operating systems).

It’s good practice to backup your computer before updating software, just to make sure if there’s an issue with the software update, you can always go back to your backed-up system!

Cyber Safety Fundamentals

Antivirus Security Scans - *Why is it important?*

Regular virus scans on your computer help to catch potential threats before they disrupt your business.

Viruses can come in many forms, from prankster tricks on your computer to ransomware which holds your computer and it's data hostage.

An active antivirus system can help to prevent potential threats from downloaded files, malicious websites or emails with infected files.

Tip: *If your antivirus software does not automatically scan emails or downloaded files, it's good practice to manually do this yourself.*

Cyber Safety Fundamentals

Computer Security Basics.

- **Trojan**
  - Malware pretends to be harmless legitimate software, or comes embedded in it, in order to trick the user and open up the gates for other malware to infect a PC.

- **Spyware**
  - This kind of malware is designed to spy on users, save their passwords, credit card details, other personal data and online behavior patterns, and send them off to whoever programmed it

- **Worms**
  - Targets entire networks of devices, hopping from PC to PC

Cyber Safety Fundamentals

Computer Security Basics.

- **Ransomware**
  - Hijacks files (and sometimes an entire hard drive), encrypts them, and demands money from its victim in exchange for a decryption key (which may or may not work, but it probably won't).

- **Adware**
  - Floods victims with unwanted ads and opens up vulnerable security spots for other malware to wiggle its way in.

Cyber Safety Fundamentals

Antivirus Security Scans - *How do I do it?*

There is more than one way to perform a security scan of your system.

You can conduct an anti-virus scan with software such as AVG, Norton, or McAfee. You can as well conduct anti-malware scans with software such as Malwarebytes.

Virus-scans can be scheduled or on demand.

If you suspect that you have a virus on your computer system, it is recommended that you contact your IT service provider as soon as possible to assist in the virus removal process – your service provider should assist in backing up your computer system, identifying the virus, removing the virus, ensuring the issue has been resolved and restore any files or programs which may have been affected.

Cyber Safety Fundamentals

Computer Security Basics.

Network Security

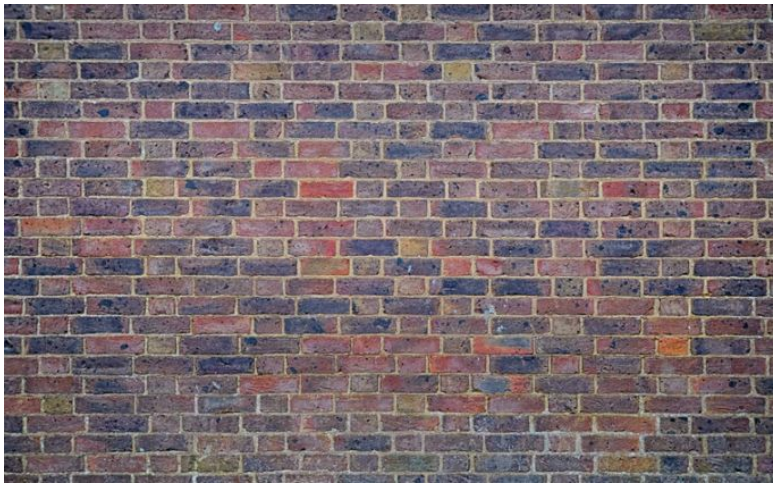
In addition to having secure computer systems, your business or organization must also have secure internet/intranet network to prevent potential hackers from being able to easily target you.

- **Password Protection**
  - Make sure that your office's wifi-connection is password protected. Networks which are not password protected can potentially have their information monitored and stolen.

- **Limiting Access**
  - IT professionals have the ability to restrict and limit access to computers. Services, folders and file s using 'permissions' and other techniques. This narrows down who is able to access this information enhances your network security.

Cyber Safety Fundamentals

- **Firewall Protection**
  - A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.



Cyber Safety Fundamentals

Computer Security Basics.

Backing Up Data - *Why is it important?*

The last thing you want to happen is for your computer to crash and not have a way of getting to your company data when you need it!

If attackers successfully target your organization's computer systems or website, the files may be corrupted or lost.

Having a backup plan for your computer information prevents disruptions in your ability to conduct business and provide your services.

Cyber Safety Fundamentals

Backing Up Data - *How do I do it?*

It is good practice to keep your computer's data backed up on a separate protected drive. This can include an external hard drive or cloud storage (data backed up online).

Depending on the scope of your business and your business requirements, backing up your data can be done either by yourself or by a professional IT service provider.

It is good practice to ensure that your backed-up data – whether it's on the cloud or on a hard drive – is secured. Encrypting your data and having secure passwords for your backed-up data will help to make sure that your information is safe.

Performing regular backups ensures that should there be a situation where your computer is disabled, you can access the data readily and minimize the impact on your business or organization.

Cyber Safety Fundamentals

Computer Security Basics.

Password Security

Your computers, websites and online accounts all require password protection to keep your information and profiles secure.

To protect passwords::

- Long Phrases
- Have two-factor authentication
- Have secure connection

https://pixabay.com/illustrations/password-app-application-business-2781614/

Email Security

Cyber Safety Fundamentals

Email Security.

Malicious emails are becoming more sophisticated and harder to detect as perpetrators develop new methods of targeting users.

A successful email attack on a business can harm productivity or bring the business to a halt. It’s not all doom and gloom!

We are providing you with a few methods, tips and tricks which should assist you in spotting malicious emails before they become a danger to you or your business.

Cyber Safety Fundamentals

Email Security.

Understanding email tactics being used to target users.

Staying calm and thinking critically is the best tool in fighting email scams. Most emails attacks are designed and structured to make you act outside of your comfort zone. Whether it's to scare, panic, or lull into a false sense of security, many methods are deployed.

Always remember the Golden Rule: Stay Calm and Carry on!

1. **Do you know the email sender?**
2. **Verify the email sender's information is accurate.**
3. **Assess the content.**
    a. Urgency
    b. Scare Tactics
    c. Unusual Demands for Money
    d. Images and Links
    e. Suspicious attachments

Cyber Safety Fundamentals

1. Is the email sender familiar to you?

First and foremost, identify if the person, company or organization is one which is familiar to you.

Have you signed up for products or services with them in the past? Are they a known person you've corresponded with or have provided your email to?

If not, this is the first step in identifying a potential malicious email. Although cold-call emails are common (especially if your business accepts public requests for inquiry), it doesn't hurt to approach a new email with a healthy dose of caution.

Cyber Safety Fundamentals

Example:

You have received an email from “Acme Marketing Agency” and they demanding that you e-transfer $1,000.00 immediately for alleged services rendered or they will call the police.

- *Have you ever had dealings with Acme Marketing Agency?*
- *Is this the first time hearing about them?*
- *Check around the office to confirm if your business or organization does have a relationship with them before responding or taking action.*

2. Double-check the email sender’s name and email address.

Double-checking the name of the sender is a good practice. It’s easy for us to casually skip over this in our day-to-day business however if you’re receiving suspicious looking email from them, this is a crucial step in assessing a potential threat.

First, check the spelling of the name of the sender. Ensure that there are no typos in the sender’s name itself.

Second, closely examine the email address of the mail sender.

Cyber Safety Fundamentals

Example

You may receive an email from “Apple Support” requesting you “Click on this link” to reset your password. If you examine the email address of the sender itself, it may give you additional clues if this email is legitimate or not. There may be typos in the email address or the email address may look suspicious itself. If the email address itself seems suspicious, copy and paste it into your search engine to check if this is indeed a legitimate email from the company or organization.

- Check the email header or the email for typos.
- Before clicking on links, hover your mouse cursor over it. If the preview text appears to lead you somewhere away from what looks like the sender’s site, do not click.
- Research online if this is a known email the sender uses.
- Contact the sender from a confirmed known address to ensure this is a genuine email that’s been sent to you.

Cyber Safety Fundamentals

3. Assess the email content.

Sometimes it’s easy to pick up on whether an email is malicious or not, other times it’s not. Perpetrators can deploy a wide-range of methods to invoke the response they want out of their potential victims.

The key to mitigating the risks is having the patience to carefully review the email content before taking any actions.

Malicious emails may attempt to appear as legitimate messages such as from government tax agencies, company support or as billing requests.

Often, illegitimate emails will use tactics to dissuade you from carefully reviewing the email content by using threatening language or prompting immediate and urgent action.

Cyber Safety Fundamentals

Urgency.

If the emailer is attempting to urge you into immediate action – more likely than not, the malicious emailer is attempting to dissuade you from carefully reviewing information and prompting you to click links, provide sensitive information, or urge you to make payments.

These types of high-urgency messages typically attempt to motivate the reader into a sense of panic. Stay calm, review the sender's email address and investigate if the email address is legitimate or not.

If you are not sure, contact the company or organization directly to confirm the validity of the email.

Cyber Safety Fundamentals

Scare Tactics.

Emailers may attempt to scare users into performing actions.

This may include clicking on links because “Your account has been compromised” or “You must pay ‘x’ amount of money” or there will be “immediate repercussions.” Caution is always advised because there is always the chance that these may be legitimate warning emails.

There are key identifiers which assist in examining whether these are legitimate emails. Review the email sender information to see if the email address is valid and use your search engine to research if the company or organization actually uses that email.

If the email is using threatening language, this is suspect, most companies and organizations stay away from threatening language when sending information about compromised accounts or accounts which have outstanding balances.

Cyber Safety Fundamentals

Unusual demands for money.

One way to identify the validity of the email is examining what kind of demands are being made if there is a payment request.

In most cases, it is safe to assume that legitimate organizations, companies or institutions will not request that you make payments in gift cards or Bitcoin. This is a common request in scam emails where payment extraction is an end goal.

If you have questions about payment requests or whether your accounts are overdue, login to your account online and check your balance, alternatively you can directly contact the company or organization and request they provide you with your account balance and method of payment.

Cyber Safety Fundamentals

Images and links.

Refrain from clicking on images and links on suspicious emails until you have been able to establish that they are safe links to visit.

Sometimes a link may say one thing but point to somewhere else completely different.

One way to identify this is using the trick of hovering your mouse cursor over the link without clicking on it. Typically when you do this, either on the bottom right or bottom left of your screen, additional information will appear which shows the true link address.

Cyber Safety Fundamentals

Email Security.

Example.

A link may say “Click on www.google.com/login to change your password” but the actually link itself may point to somewhere else. This is a strong indicator that the link is not safe to visit. Another way to check a link is to carefully use your mouse to “right-click” and copy the link address, then go to your search engine and paste the link in there to search (be careful not to enter the link and visit the site). The search results may provide additional insight into whether the link Is legitimate or not.

Cyber Safety Fundamentals

5. Suspicious attachments.

There are times when scammers or malicious players try to send an email which includes an attachment file, encouraging you to open and perform tasks on it.

Sometimes emails may arrive from known contacts, however they may have been compromised and are forwarding the virus attachment automatically.

If you receive an email which you believe to be suspicious and includes an attachment, it is recommend that before downloading or opening the file, to scan it with anti-virus software.

If you have received a suspicious email from someone you are familiar with, the best course of action is to wait before downloading the file and contact the person directly to verify the that the file is safe to download and view.

Cyber Safety Fundamentals

Set Your SPAM Filter.

Finally, make sure that you have your SPAM filter set up on your email account. What's a SPAM filter? A SPAM filter helps to sort out legitimate emails from potentially malicious messages. You can learn more about SPAM filters here: **https://www.pcmag.com/encyclopedia/term/51792/spam-filter.**

SPAM filters are a great way to quickly lower the number of 'junk' email you receive, but also make sure to check in ever so often in-case a legitimate email does get sorted into here.

Cyber Safety Fundamentals

Wrapping Up.

There simply isn't a sure-fire guarantee that you will not be targeted from a potentially malicious email, unless you don't have an email. However, with the help of these techniques and staying vigilant, you'll be in a good spot to detect potential threats and protect yourself and your business from threats.

If there is a virus or threat to your technical threat to your business or have fallen victim to an email scam, it is recommend that you contact your local authorities and as well contact the Canadian Anti-Fraud Centre for further guidance: **http://www.antifraudcentre-centreantifraude.ca/reportincident-signalerincident/index-eng.htm**.

Online Safety

Online browsing
Social Media

Cyber Safety Fundamentals

Much of the same techniques which we've already discussed in identifying and safeguarding from social engineering attacks also apply to online safety.

Online safety should be a part of your organizational IT policy, these are typically labelled as "Internet Usage Policies." These policies provide guidelines and education for staff as to what is acceptable use of internet on company computers and networks as well as guidance to what should be done if there is a security risk.

Cyber Safety Fundamentals

IT professionals can help to restrict access to certain range of websites or specific websites. *For example, all gambling websites can be restricted on a computer or network.*

Employees should be informed as to what kind of information is acceptable to post online and where. A social media policy can also assist staff in understanding their roles and what is permissible online posting habits.

Cyber Safety Fundamentals

- Only visit legitimate or verified websites.
- Do not give out sensitive organizational information online if requested.
  - If requested, go through the process of verifying the validity of the request and the legitimacy of the asker. Always be 100% sure.
- Ensure that complex passwords are used for online profiles.
- Before clicking links, check URLs to ensure websites and links are what they say there are.
- Only download files and programs from trusted sources.
  - Always perform a virus scan on downloaded files.
- If you stumble onto a website which is employing what you suspect may be an attack, do not panic. Close the browser, disconnect from the internet and perform a virus scan. If concerns remain, contacting an IT professional can help to ensure the safety of your system.

Wrapping Up.

Cyber Safety Fundamentals

Wrapping up.

One of the greatest tools which attackers deploy against individuals, businesses and organizations, whether it's via email or online attacks, is to get you panic and make out-of-character rash decisions.

Whenever you are ever suspicious of an email, website or correspondence, your greatest tool to in defence is taking a deep breath and thinking critically.

- Review the source.
- Review the content.
- Do the research.

If you follow these steps, you will likely be able to identify threats before they become reality to your organization.

Cyber Safety Fundamentals

What is recommended for your organization to have in place:

- IT Policy.
- Internet Usage Policy.
- Social Media Policy.

These policies can be created with your management team, HR and with the assistance of an IT professional.

Cyber Safety Fundamentals

Wrapping up.

At the end of the day,

there simply isn't a sure-fire guarantee that you will not be targeted from a potentially malicious email or online social engineering attack.

However, with the help of what we've discussed today and staying vigilant, you'll be in a good spot to detect potential threats and protect yourself and your business from threats.

If there is a virus or threat to your technical threat to your business or have fallen victim to an email scam, it is recommend that you contact your local authorities and as well contact the Canadian Anti-Fraud Centre for further guidance.

Cyber Safety Fundamentals

Wrapping up.

Resources:

https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-eng.htm

http://www.chamber.ca/media/news-releases/170403-canadian-businesses-lose-billions-of-dollars-to-cyber-crime-each-year/

https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

https://www.imperva.com/learn/application-security/social-engineering-attack/

https://geekflare.com/understanding-cybersecurity/

https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx#s4

Questions and Discussion

Contact:

Blue Sky Net
Jerry Poliszczuk
ICT Community Outreach Coordinator
Email: jerry.poliszczuk@blueskynet.ca