On-line and email usage Security tips

We are continuously adopting new and innovative technologies and spending more of our time online. The thirst for computers, smartphones, and Wi-Fi seems to have no limits. At home, at work and at school, our growing dependence on technology, coupled with increasing cyber threats and risks to our privacy, demands greater security in our online world.

Cybercriminals do not discriminate; they target vulnerable computer systems regardless of whether they are part of a government agency, large company, small business, or belong to a home user. There are however steps you can take to minimize your chances of an incident:

- **Passwords:** Set strong passwords, change them regularly, and don't share them with anyone.
- **Updates:** Keep your operating system, browser, and other critical software optimized by installing updates.
- **Communication:** Maintain an open dialogue with your friends, family, colleagues and community about Internet safety.
- **Limit information:** Use privacy settings and limit the amount of personal information you post online.
- **Be cautious** about offers online – if it sounds too good to be true, it probably is. Be wary of claims of quick riches.

Copyright infringement

Copyright infringement occurs when you use or distribute information without permission from the person or organization that owns the legal rights to the information.

An image or cartoon on your website or in a document, illegally downloading music, and pirating software are all common copyright violations. While these activities may seem harmless, they could have serious legal and security implications.

How do I know if I have permission to use something?

- If you find something on a website that you would like to use (e.g., a document, a chart, an application), search for information about permissions to use, download, redistribute, or reproduce. Most websites have a "terms of use" page that explains how you are allowed to use information from the site.

- There may be restrictions based on the purpose, method, and audience. You may also have to adhere to specific conditions about how much information you are allowed to use or how the information is presented and attributed. If you can't locate the terms of use, or if it seems unclear, contact the individual or organization that holds the copyright to ask permission.

What are the consequences for using illegal downloads?

- **Prosecution** - When you illegally download, reproduce, or distribute information, you risk legal action. Penalties may range from warnings and mandatory removal of all references to costly fines. Depending on the severity of the crime, jail time may also be a possibility. Additionally, to offset their own court costs and the money they feel they have lost because of pirated software; vendors may increase the prices of their products.

- **Infection** - Attackers could take advantage of sites or networks that offer unauthorized downloads (music, movies, software, etc.) by including code into the files that would infect your computer once it was installed Because you wouldn't know the source or identity of the infection or even if you have one, it is not easily identify or removed. Pirated software with hidden Trojan horses is often advertised as discounted software in spam email messages.

Email Safety Tips

Email has become an essential tool for communicating, which is why it is so popular with scammers, cybercriminals and advertising companies. In order to protect ourselves from phishing scams and malware, it is essential that we learn how to safely manage our mail.

Spam is another term for junk email or unwanted email advertisements. Today, the majority of emails are spam. That's because it's very easy and inexpensive for a spammer to send an email to thousands of people at the same time, and they can do it anonymously. Phishing scams and malware are often included in spam, so it is important to be able to effectively manage the spam we receive in our inbox.

- **Use a Spam Blocker.** A spam filter can greatly reduce the amount of spam that ends up in your inbox. Unfortunately, even with a spam blocker, some spam may still get through.

- **Don't Reply to Spam.** You may be tempted to reply to a spam email or click on a link within the email to unsubscribe. This may work with legitimate emails that you have subscribed to; however, spammers will

rarely honor these requests. In fact, by replying or clicking on a link, you are confirming to the spammer that your email address works, and you may end up getting more spam.

- **Turn Off Images.** An email may contain images that the spammer can track. When you open the email, the images will load, and the spammer will be able to tell that your email address works, possibly resulting in even more spam.

- **Turn Off Your Preview Pane** (if your email service has one). It is impossible to avoid viewing spam when your email automatically displays it in your preview pane. Once you view a spam message it may actually lead to receiving more spam. Therefore, you will need to weigh the convenience of using your preview pane with your desire to avoid spam.

- Email Scams – Remember, if it's too good to be true, it probably is. Popular email scams include work-at-home offers, weight-loss claims, debt-relief programs and cure-all products.