pti Public Technology Institute ICMA

10 Simple Steps to Online Safety

How to protect yourself and emphasize the importance of cybersecurity in the workplace:

1. **Passwords still matter.** Using different passwords that contain and include at least 8 characters with numbers and symbols. Try and come with a formula where you can remember them too. For example, you may use and old address as a starter or transpose a letter for a number or symbol. Passwords should not begin with a capital letter, and underscore is a good way to separate a bunch of numbers.

2. **Use Multiple Passwords.** By using multiple passwords for different accounts, you spread the risk of having one breach expose you to everywhere you have a login account. Too many passwords to remember? Consider using a "password manager" like LastPass or Dashlane. Most offer free versions that one can try out. While these systems require a complex master password, password managers do the rest. You can elect to have them assign complex random passwords and most have an autofill feature that fills in the necessary fields automatically. Another advantage is most password managers remember and recall passwords and payment information across your devices if you so choose. This includes PC, laptops, and all your mobile devices.

3. **Think Before You Click.** Ransomware and phishing attacks have increased dramatically the past 2 years. Many of these attacks can be traced to employees clicking and opening attachments. Before you open an attachment are you sure it is from a person or entity they say they are? Do you see suspicious signs like misspellings, using a salutation such as "dear customer" instead of your name, a return URL/address that is different from the senders? For example, if you receive something that appears to be from your bank, is the URL taking you to the bank or is it directing you somewhere else. It's always best not to click on such emails regardless of how real they look. Instead simply go directly to the company's site and see if there is any real issue for you to resolve. Finally, if in doubt always contact your IT folks as they have ways of checking authenticity without risk to others.

4. **Limit Address Book Entries.** It is shocking to learn how many professionals use their mobile device address books to store credit card numbers, passwords, family social security numbers and birthdates. As temping as it is don't use your mobile device's directory as your personal information database! Most cyber breaches attack your address books and yes, these same rogue software programs are programmed to search for this type of information in addition to all your contacts. Remember, the bad-guys goal is to exploit ever bit of information they can and use it to cause further havoc which could lead to identity theft, use passwords to enter systems to obtain further a perhaps more important information.

5. **Update your Devices.** Computer and mobile device manufacturers are routinely updating their operating systems to help improve performance as well as actively addressing known security vulnerabilities. It should go without saying, make sure you not only have the best virus and malware protection – but it is updates in real-time to gain maximum protection.

6. **Avoid Public WI-FI.** It is always tempting for on-the-go-people to connect every time they see a WI-FI hotspot. There are plentiful offerings at airports, trains, coffee shops, hotels, and conferences. Unfortunately, public Wi-Fi (free or not) can easily be exploited by the bad-guys who can “see” what you are logging into with not much effort and be able grab your passwords. Never conduct business in public places offering Wi-Fi that requires passwords which might include logging into your office or your bank. Consider having your own mobile hotspot offered by all wireless carriers. Even though you are still connecting via Wi-Fi it is far more difficult to snoop and the data is usually encrypted and ultimately converted to more secure cellphone frequencies.

7. **Secure Your Cloud.** The cloud stores huge amounts of information and serves as a free storage locker for your documents, photos, messages, and more. No matter what cloud provider or service you use, make sure you do your due diligence on their security practices. If they can’t easily and quickly tell you how your data is secured, odds are it isn’t. Also, for any accounts used to access your government’s data, make sure you have strong passwords and only access it via a computer you own or trust. If you access your cloud on an infected device, a hacker could potentially learn your password and use it later on without your knowledge.

8. **Back Up Your Data.** Not regularly backing up your files exposes you to the risk of losing that information. By storing the backup information offsite on a daily and weekly basis, you minimize the loss of information.

9. **Read Your Organization’s Acceptable Use Policy.** Every organization should have an acceptable use policy that is documented, reviewed, and maintained on a regular basis. Acceptable use policies typically include acceptable internet usage, how remote workers can access the network, social media regulations, and how to report security incidents.

10. **Educate Yourself.** Cybersecurity is not just a federal or private sector issue. It is a whole community issue that requires partnerships, vigilance, and proactive efforts on every level of government. To ensure that your municipality has adequate security measures in place, search for a training course that educates you on how to protect your organization and safeguard citizens’ records.

International City/County Management Association (www.icma.org)
ICMA, the International City/County Management Association, advances professional local government through leadership, management, innovation, and ethics. Our vision is to be the leading professional association dedicated to creating and supporting thriving communities throughout the world.

Public Technology Institute (www.pti.org)
Created by and for cities and counties, the not-for-profit Public Technology Institute promotes innovation and collaboration for thought-leaders in government, and advances the use of technology to improve the management and delivery of services to the citizen.