COVID-19
Cyber Security Update
October 14, 2020

Edmonton

With many employees continuing to work from home, it is important to keep our guard up to maintain our online security. Recent cybercrime trends show us that criminals are looking to profit from individuals in any way that they can. City staff continue to be important in protecting and securing our online environment. Please continue to do your part to protect the City's information and technology by following these practices:

Phishing by Email and Text Message

Attackers are using tactics that take advantage of the COVID-19 pandemic. This includes offers of miracle cures, advance COVID news, special package deliveries and food deliveries. If you suspect that you have received a fraudulent message by email or text message, the best course of action is to delete it and carry on with your normal activities. Some common indicators to help you determine if a message is fraudulent:

- Is this an unexpected message, or from an unknown address?
- Does the message use threats, incentives, or communicate a sense of urgency?
- Does the message use poor spelling, capitalization or grammar?
- Does the message entice you to click, download or install files?
- Does the message link to an unrecognized or misspelled website?

In the event that you have clicked on an illicit link or downloaded a suspect file, please contact Inside Information at (780) 944-4311 to report a potential cyber security incident.

Fraudulent Phone Calls

Criminals continue to contact staff by phone and are using technologies to hide the phone number they are calling from. If you suspect you have received a fraudulent phone call, do not provide the caller with any information or contact details, and hang up.

The City cannot stop these kinds of calls coming through the corporate phone system or the cell phone systems. If you receive a call or voicemail that you think is a phone scam, we encourage you to report this activity to the Canadian Anti Fraud Centre.

The best response to one of these fraudulent phone calls is to hang up.

Password Security and Identity Theft

With an increase to identity theft and business email compromise, it is always a good idea to ensure that we are keeping our digital accounts safe and secure. Below are some best practices for consideration:

- The longer your password, the more difficult it will be for an attacker to obtain. Consider using a small sentence or a phrase that means something to you personally.
- It is best to use the entire keyboard and not just the letters, numbers and characters that you use most often.
- Passwords should be unique for each account or website that you access. If cyber criminals gain access to just one of your passwords, they will attempt to test them against all other services.

Ensure that you follow City processes and procedures to verify the identity of an individual before making payments, changes to financial or bank information, or granting access to any City systems. If you suspect that someone is impersonating another individual or identity theft is occuring, please contact Inside Information at (780) 944-4311 to report a potential cyber security incident.

Working Remotely with City Assets

Corporate devices and your Corporate login IDs are intended for work purposes only. Please remember:

- City assets are intended for use by City employees.
- Your City devices should be locked and secured while you are not using them.
- Your login IDs should be logged off while you are not using them, or your session should be locked.

Working Remotely With Google Files

While working from home, all staff need to be cautious about accessing and working with Google files. Please remember:

- Do not download corporate Google files to your personal computer or device.
- Be aware of who you are sharing your files with.
- Ensure that you are providing the minimal amount of access required.
- Remove any access that is no longer required.

Keep Your Work and Personal Devices Up To Date

When working from home or in the office it is important to keep all of your devices up to date. This includes any phone, tablet or computer that you may be using to access our corporate systems and data. These updates are vital because they provide security patches, operating system updates, and performance enhancements to your devices and applications.

To ensure that this is happening, please take a moment to check for available device updates, and confirm that your device will update automatically. If you have questions or concerns, please send an email to Open City & Technology's Voice Mobility team at device.security@edmonton.ca.

Video Conferencing

The City of Edmonton Corporate Information Security Office has assessed the Zoom Video Communications (Zoom) platform and strongly recommends that City employees refrain from using Zoom on the devices they work from.

The approved City of Edmonton video conferencing platform is Google Meet. There are a number of reasons we choose Google Meet over other platforms, including secure end-to-end encryption and Google's user policy prohibiting the sale of enterprise customer data to third parties.

Google Meet is free for anyone to use and meetings with external stakeholders should be encouraged on this platform. However, if a meeting must be held on Zoom or another platform, please follow these precautionary steps:

- Do not make meetings public and use passwords for access to meetings if possible.
- Do not share links for meetings publicly.
- Only allow meeting hosts to have the option to share their screens with other participants.
- If you have a Zoom username and password enable two-factor authentication.
- Ensure that you are using the most recent version of the application.

Users should be aware that the City only supports video conferencing on Google Meet and cannot assist if there are technology issues on another platform.

If you are recording any meeting, please inform all participants prior to commencing the recording. If you have questions regarding privacy and meetings, please contact the Corporate Access and Privacy Office at foip@edmonton.ca.

If you need assistance using Google Meet, contact Inside Information at (780) 944-4311.

Cyber Security Awareness Presentation

The Corporate Information Security Office provides guidance and awareness in Cyber Security best practices. To book a 15-minute information session for one of your upcoming team meetings, please contact us at iSecurity@edmonton.ca.