Cyber Security Awareness

Alicia Fugate
ITMD
City of Milwaukee

What is cyber security?

- **Cyber security** is a term used to describe the techniques practiced to protect computers, networks, servers, programs and data from unauthorized access
- This is a **shared responsibility** among all City staff, do your part by learning more about best internet and Cyber security practices and being more aware of threats and vulnerabilities.

Computer Virus

- A virus has the potential to cause unexpected or **damaging** effects, such as **harming** the system software by corrupting or **destroying data.**
- Viruses are designed to **spread** to other computers and have the ability to **replicate** themselves

Phishing

Forward suspicious emails to emailadmins@milwaukee.gov

- Phishing is the fraudulent attempt to obtain sensitive information such as usernames, password and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.
- Spear Phishing is a phishing attempt aimed at a specific individual.
- According to the Webroot Threat Report, nearly 1.5 million new phishing sites are created each month.

Phishing Example

Forward suspicious emails to emailadmins@milwaukee.gov

From: Outloook.com [mailto:24975bsn-kqv--2497524975@birch.nocdirect.com]

Sent: Monday, May 07, 2018 11:16 AM

To: Olson, Nancy <Nancy.Olson@milwaukee.gov>

Subject: Your account is 99% full now

Importance: High

Microsoft-Outlook

Your mailbox is 99% full

This message was sent to nancy.olson@milwaukee.gov because your mailbox is 99% full

Once your mailbox is full, you won't be able to send or receive email.

We notify you about this, to help regain your access.

Phishing Example

Forward suspicious emails to emailadmins@milwaukee.gov

Take action to keep getting emails

From: Lloyd from Microsoft <customercare@mcs-office.com>
Sent: Friday, September 6, 2019 9:41 AM
To: Olson, Nancy <Nancy.Olson@milwaukee.gov>
Subject: Take action to keep getting emails

Your Office 365 is flagged for login activity

Our records indicate that it has been more than 15 days since you logged into Office 365 through the web. For security reasons, this account will be locked due to inactivity.

To keep using your email, you must confirm that NOlson@milwaukee.gov is still in use by using the activation button below.

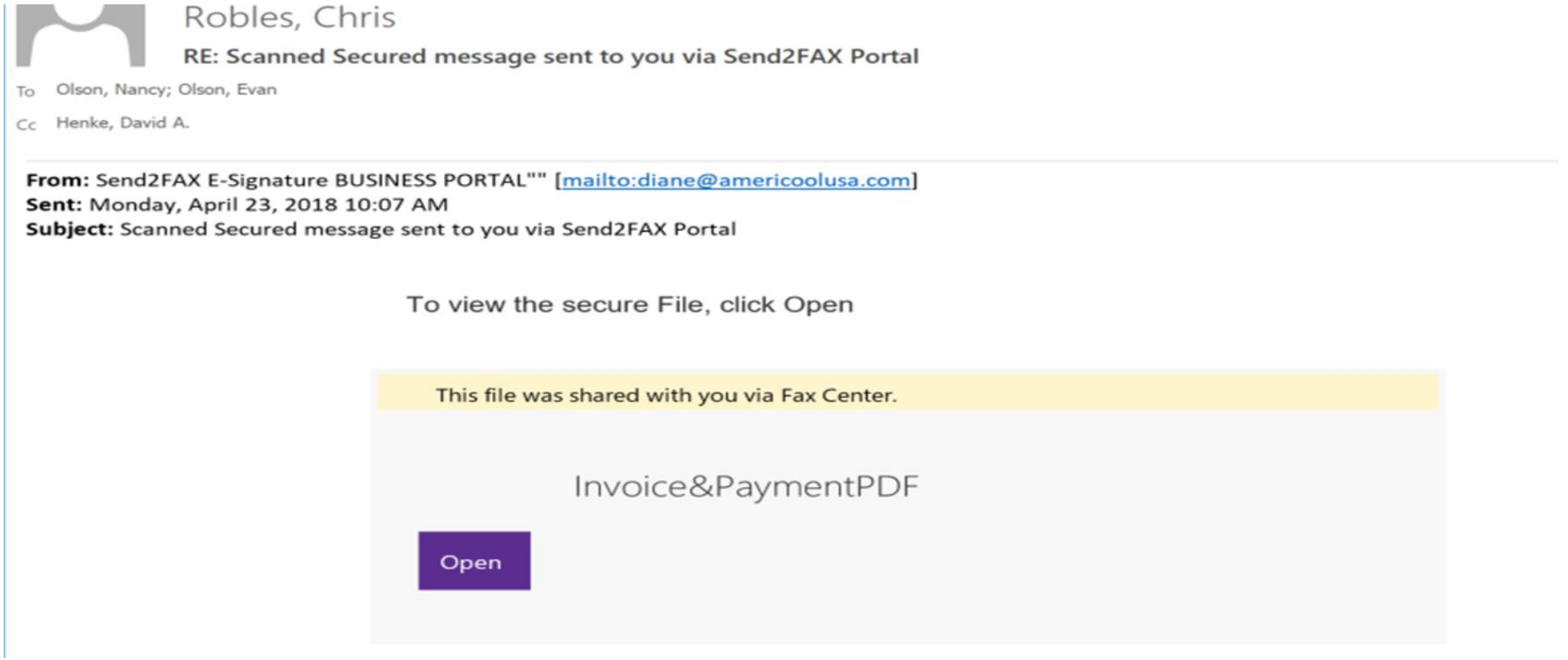
Mark As Active

You should use this button only if you want this account to remain active. If you no longer work at the company, please ignore this email.

Thanks for using Office 365!

Phishing Example

Forward suspicious emails to emailadmins@milwaukee.gov



Robles, Chris

RE: Scanned Secured message sent to you via Send2FAX Portal

To Olson, Nancy; Olson, Evan

Cc Henke, David A.

From: Send2FAX E-Signature BUSINESS PORTAL"" [mailto:diane@americoolusa.com]
Sent: Monday, April 23, 2018 10:07 AM
Subject: Scanned Secured message sent to you via Send2FAX Portal

To view the secure File, click Open

This file was shared with you via Fax Center.

Invoice&PaymentPDF

Open

Phishing Example

Forward suspicious emails to emailadmins@milwaukee.gov

From: Grant F. Langley [mailto:shérifff@countiiesgov.com]
Sent: Wednesday, July 24, 2019 10:12 AM
To: Owczarski, Jim
Subject: Payroll Update

Jim,

Please email a form to fill for Employee direct deposit form change and want it effective for next pay check.And who do I return the completed form to?. Do i fax it or return it as email.

Thanks.

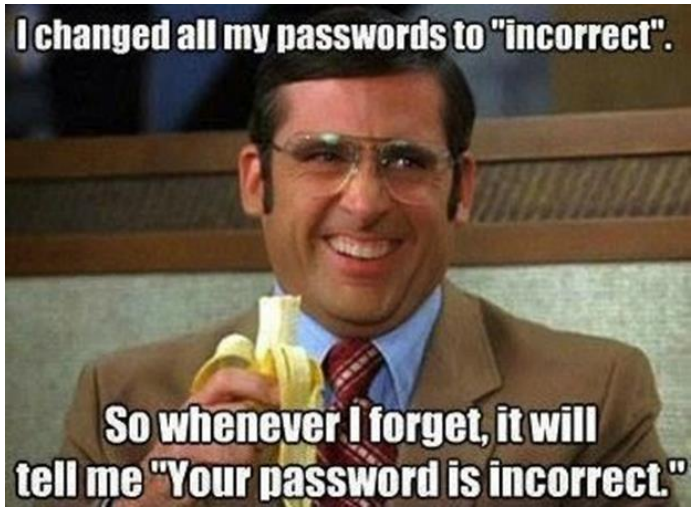
Grant F. Langley

What can you do?

- Choose strong passwords
- Secure your workstation
- Take the time to think and read before you click
- Be more aware of threats lurking in your email
- Don’t use any external devices that don’t belong to you
- Save your work

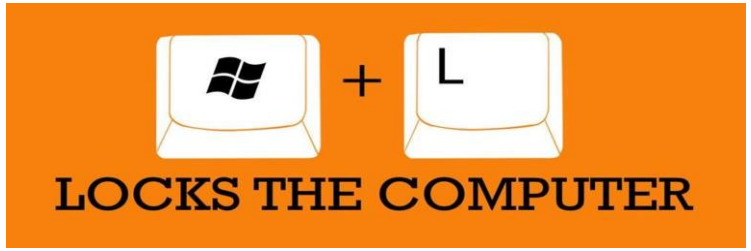
Passwords/Pass-phrases

- The password must be a minimum of 8 characters in length, contain a combination of lowercase letters, capital letters, numbers and special characters (e.g. ! # $ % ^) and cannot contain the user's name. (per password policy in MINT)
- Always change all of your passwords after your computer/device fails or becomes infected. This includes any personal accounts you logged into from that device
- Do not share your passwords with anyone, Including when making a RITS request, in a text or email



Lock Up!

- Don't leave your computer unsecured when you are not there
- This is especially important to those working in public facing positions
- Shut down your computer if you anticipate being away from your workstation for more than a day

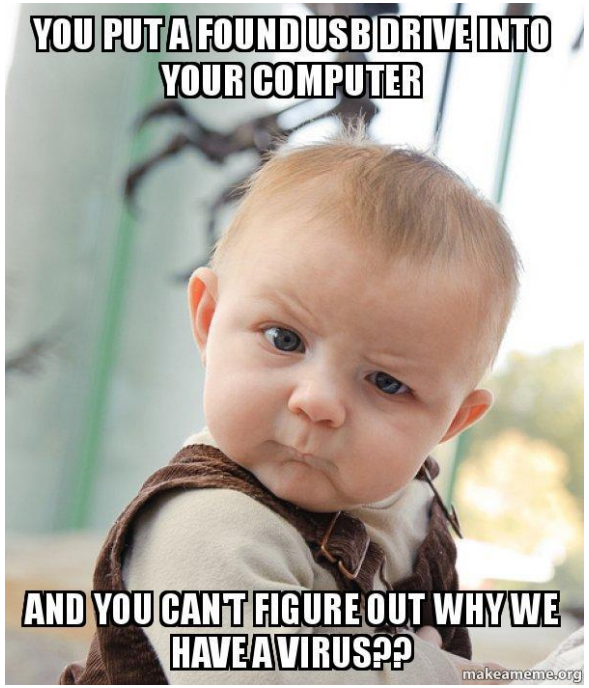


City Email

- **Do not use your personal email address for business/work** purposes
- Be mindful- City email is **subject to public records requests**
- If any user receives a suspicious email (e.g. phishing, scam, etc) it should forwarded it to **emailadmins@milwaukee.gov**

External Devices

- Any disk or **thumb drive** connected or inserted into your computer could become infected with a **virus.**
- Don't plug any devices(flash drives, disks, flash memory..) into your computer that do not belong to you.



Saving Your Work

- All data should be saved on the **network drive** such as the I:drive or J:drive
- **Do not** save your work to **"my documents"** or to your **desktop**

What ITMS does to protect you from cyber threats

- Regular security and software updates
- Block web content that could expose the city to potential threats
- Help desk for concerns, dial **2777**
- Provide email support for suspected threats **emailadmins@milwaukee.gov**

Software Updates

- All software updates to your workstation are performed by ITMD.
- Best practices: Save your documents, close all applications, and log off at the end of the day.
- Once updates have been applied your computer may require a restart.

Cloud Computing

- **City Employees are NOT to open cloud services accounts** or enter into cloud service contracts for the storage, manipulation or exchange of **city-related communications or city-owned data without the IT Management/CIO's input.**
- **Personal** cloud services accounts may not be used for the storage, manipulation or exchange of **City-related communications or City-owned data.**
- Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including **termination of employment**.

Common symptoms of a virus &what to do about it

- Erratic computer behavior (freezing, cursor is unresponsive…)
- Frequent computer crashes
- Pop-ups from anti-virus software

Action to take:

- Enter a RITS ticket if possible or call

ITMD at 2777 **unless you have your IT support(Treasury, MPD,MFD, Municipal Court…) contact them first.**

What does this mean to you?

- Use your best judgement and practice common sense
- If it doesn't look or feel right, don't click it!
- Always check the sender on your emails
- If you think your computer has been infected **call 2777 or enter a RITS ticket unless you have your IT support(Treasury, MPD,MFD, Municipal Court…) contact them first**
- If you receive a suspicious email, forward it to **emailadmins@milwaukee.gov**
- Remember **cyber security is a shared responsibility, each of us has a role to play**