IM@WORK FOR MY TOWN: BEST PRACTICES THROUGH THE INFORMATION LIFECYCLE

Module 2.3: IM Best Practices - Receiving

Lori Collins,

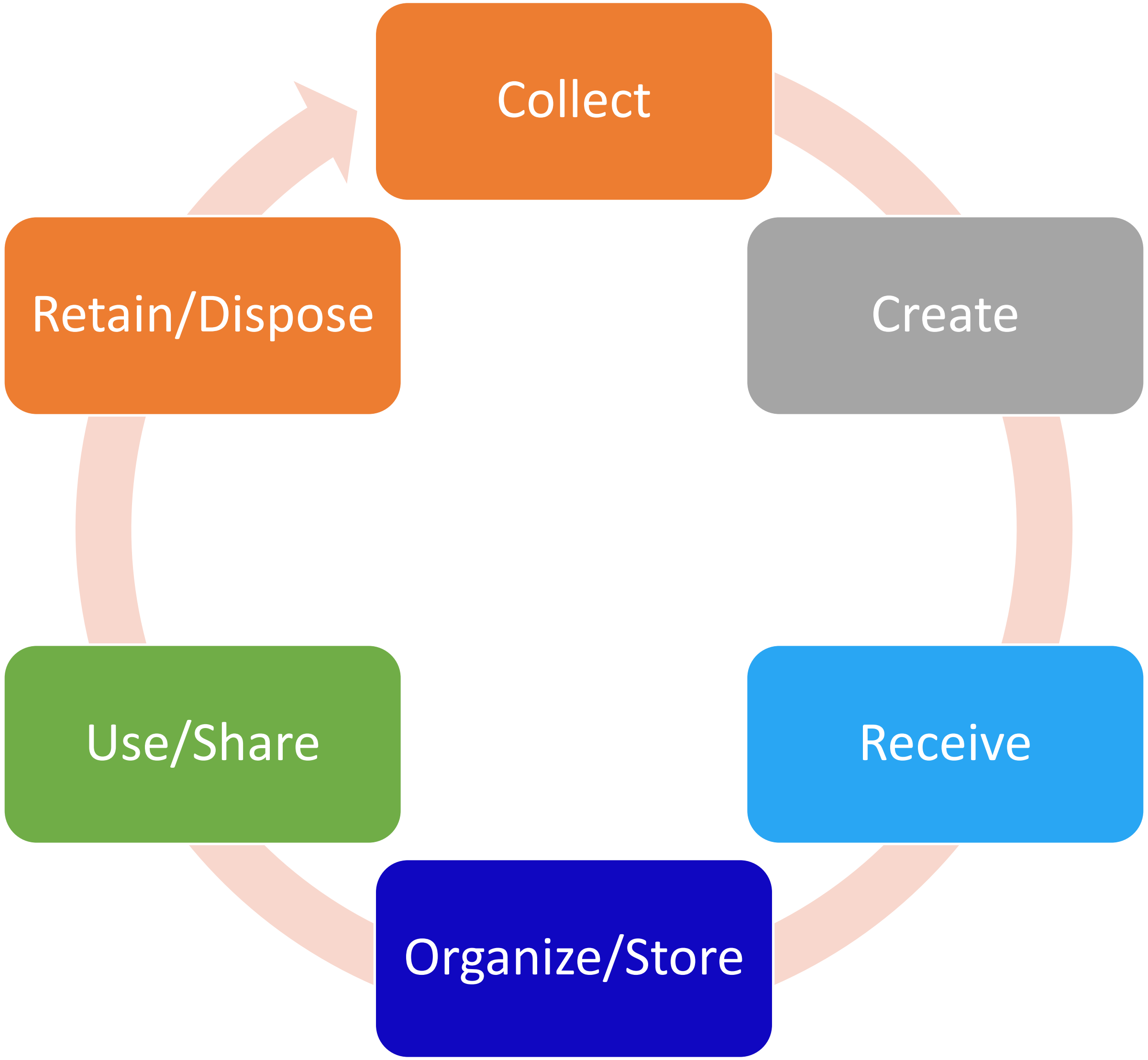
Instructor, Information Management Post Diploma

cna

Welcome to Module 2.3: Receiving

- **In Module 2.3 you will learn to:**
  - Identify when receiving of information occurs and potential sources/formats
  - Identify risks to information at the point it is received
  - Understand phishing

The Information Life Cycle



Collect

Create

Receive

Organize/Store

Use/Share

Retain/Dispose

Receiving Information

Information is received by the Town through a variety of channels including regular mail, courier, email, text messages or other messaging technologies

Information may be provided verbally in person or via phone or other technologies (e.g., Skype or Microsoft Teams)

Often is driven or flows from an external source (e.g., taxpayer)

May initiate a process or service and creation of new records (e.g., new permit)

Some information the town collects is personal or confidential. This means that it needs to be protected at all stages

There are many potential risks when receiving information!

College of the North Atlantic

Receiving Information

Risks to receiving information include:

- Information may be unsolicited and waste time
- Information received electronically via email, text or other messaging technologies may contain malware or viruses that risk information loss, cyber attacks or ransomware
- Information may not be sent to the right person to deal with an issue, complaint or request

College of the North Atlantic

Receiving Information

- We receive information as a regular part of our day-to-day work. This information can come from many different sources and in many different structures.
- When information is received it should be quickly analyzed to decide the best way to use and store it.
- When information is received it should be analyzed to identify if it is considered transitory and if it should/can be disposed of.

College of the North Atlantic

Transitory Records

A record of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record

Examples of Transitory Records

- Phone messages
- Appointment Calendars
- Convenience Copies
- Publications For Mass Distribution
- Drafts
- Working Copies
- Supporting Information
- Routing Sli

Receiving Information

- Records received by Town users will apply best practices for the protection of information
- Ensure records are routed to the authorized and intended person
- Follow established practices for receiving (e.g., date and time stamp physical records if this is your practice)
- Have a process to deal with content received via social media/messenger apps
- Classify and store information as soon as it is received

Receiving Information

- When in doubt, Check it out! Town users should verify that sources of information are trusted:
  - Go back to a previous email
  - Visit an official website
  - Person to person contact (e.g., phone or direct messaging to known accounts) as needed.

College of the North Atlantic

Phishing

When receiving or collecting electronic information, be aware of the potential for Phishing.

Phishing is a type of fraud that uses deceptive emails, websites and/or text messages to gather personal, financial and confidential information for fraudulent and/or unauthorized purposes.

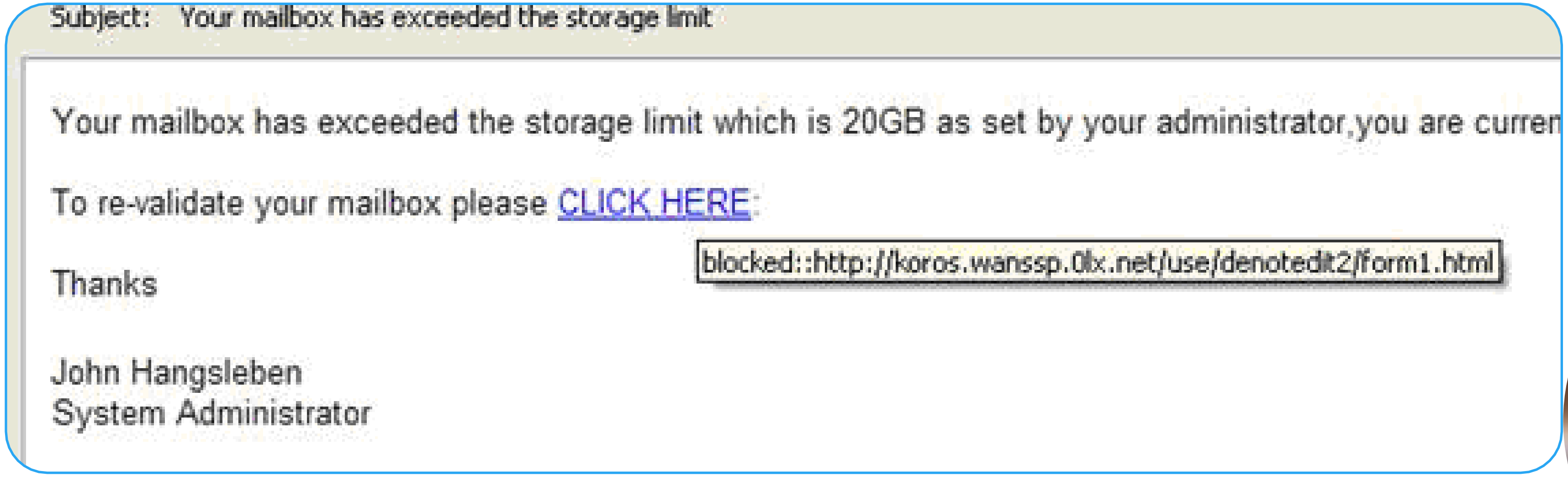
- Never click on links or attachments in e-mails from unknown sources
- Never disclose your work usernames and/or passwords
- Never use your work
for personal use

Phishing

- **“Spear phishing”** is an email targeted at a specific individual or department within an organization that appears to be from a trusted source
- Perpetrators profile victims then send a message that the victim may assume to be legitimate
- This information may have been obtained through another breach or through social media
- It may be because they know where you bank, an online store where you shopped or even because they know your kids play a sport
  - Open your discount from xyz…
  - There is a problem with your account
  - You have been chosen to receive a reduced rate on your insurance

Phishing: How to Recognize it?

- Only click on email links and attachments from known, trusted and verified sources
- Verify the authenticity of the link/website address before you select it. You can do this by moving your mouse over the link to reveal the actual address



Subject: Your mailbox has exceeded the storage limit

Your mailbox has exceeded the storage limit which is 20GB as set by your administrator,you are curren

To re-validate your mailbox please CLICK HERE:

blocked::http://koros.wanssp.0lx.net/use/denotedit2/form1.html

Thanks

John Hangsleben
System Administrator

College of the North Atlantic

Phishing: How to Recognize it?

- Check the spelling and other characteristics in the address itself

Correct Address	Example of a Phishing Address
www.royalbank.com	www.rbcc.com
www.facebook.com	www.facebokk.com
www.visa.com	www.vsa.com
www.mun.ca	www.mmun.ca

- Use your search engine to research an unfamiliar website

Phishing: Examples

- **Phishing**:
  - *“We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity…”*
  - *“During our regular verification of accounts, we couldn’t verify your information. Please click here to update and verify your information…”*
  - *“You have won a prize, contest, etc. please respond…”*
  - *“Someone you know needs a transfer of funds immediately because they are stranded…”*

College of the North Atlantic

About IM@Work For My Town

MODULE 1: IM BASICS

MODULE 2: BEST PRACTICES

2.1: COLLECTION

2.2: CREATION

2.3 RECEIVING

2.4: ORGANIZE/STORE

2.5: USE/SHARE

2.6: RETAIN/DISPOSE

MODULE 3: ROLES AND RESPONSIBILITIES

References

- *Cyber Security Awareness*, Office of the Chief Information Officer, Government of Newfoundland and Labrador: https://www.gov.nl.ca/exec/ocio/security/cybersecurity/
- Get Cyber Safe, Government of Canada: https://www.getcybersafe.gc.ca/en/resources/7-red-flags-phishing

College of the North Atlantic

CONTACT US

Ashley Sheppard
Communications Coordinator, PMA

Email: Ashley@pmanl.ca

Tel: 709-726-6405

Lori Collins

Instructor, Information Management Post Diploma

E-mail: Lori.collins@cna.nl.ca
Tel: 709.728-6726

Rod Hynes

Municipal Access and Privacy Analyst, ATIPP Office, Department of Justice and Public Safety,

Rhynes@gov.nl.ca
E-mail: name@cna.nl.ca
Tel: 709.123.4567