MCIT
Minnesota Counties Intergovernmental Trust

LOSS PREVENTION

Quick Review of Data Security

PHISHING AND SOCIAL ENGINEERING

WHAT IS SOCIAL ENGINEERING?

Phishing and social engineering attacks attempt to trick users into revealing private information or passwords, access to secure systems or areas.

RECOGNIZING ALL TYPES OF SOCIAL ENGINEERING

- **Requests require fast response or crucial time window:** Social engineering attacks rely upon a person not asking for confirmation or checking with others prior to acting.
- **Threats:** This goes along with rushed requests. There are often negative consequences implied if the request is not completed quickly. Threats of fines, denied access, missed opportunities for easy money or employment termination are common.
- **Unsolicited messages:** Social engineering attacks are not typically in response to a request or other previous communication. Receiving an unsolicited communication should raise suspicions.
- **Requests for sensitive information:** Most attacks ask for passwords, login information, Social Security numbers, bank account numbers, credit card information or other data that is typically kept private or confidential. Requests for this information from any source should be treated with suspicion.

(Over)

MCIT
Minnesota Counties Intergovernmental Trust

LOSS PREVENTION

Quick Review of Data Security

PHISHING AND SOCIAL ENGINEERING

WHAT IS SOCIAL ENGINEERING?

Phishing and social engineering attacks attempt to trick users into revealing private information or passwords, access to secure systems or areas.

RECOGNIZING ALL TYPES OF SOCIAL ENGINEERING

- **Requests require fast response or crucial time window:** Social engineering attacks rely upon a person not asking for confirmation or checking with others prior to acting.
- **Threats:** This goes along with rushed requests. There are often negative consequences implied if the request is not completed quickly. Threats of fines, denied access, missed opportunities for easy money or employment termination are common.
- **Unsolicited messages:** Social engineering attacks are not typically in response to a request or other previous communication. Receiving an unsolicited communication should raise suspicions.
- **Requests for sensitive information:** Most attacks ask for passwords, login information, Social Security numbers, bank account numbers, credit card information or other data that is typically kept private or confidential. Requests for this information from any source should be treated with suspicion.

(Over)

RECOGNIZING PHISHING SCAMS

- The sender's address is in a different format than the rest of the organization's (e.g., all e-mails within the organization follow the format of "firstname.lastname@co.county.mn.us" but the message claiming to be from someone within the organization is different).
- There are frequent misspellings and poor grammar. Many attacks originate in non-English speaking parts of the world.
- The message asks users to click on links or open attachments.
- If anything sounds too good or too bad to be true (e.g., "Claim your tax return now" or "We have your kids.")
- The message includes outrageous or sensational headlines or imagery that entices you to click on them.
- The message is in a spam or junk e-mail folder. Many IT departments and e-mail providers have filters that automatically screen spam messages. If a message is in the spam folder, it can be a clue that it may not be legitimate.
- There is a vague greeting and sender. Often bulk phishing attempts are not directed to individual people. Messages may start with "attention" or another generic word or phrase. Similarly, messages that end with a title or vague location should be viewed with suspicion (e.g., "web administrator or "help desk").
- Hovering the mouse cursor over the link shows a different Web address than the indicated link.

PREVENTION

If a message has one or more of the elements above, you should:

- Contact IT.
- Follow IT directions.
- Do not open the message, click on any links or items or follow instructions in the message, such as sending confidential information or passwords.
- Forward any requests for private information to the responsible authority for your organization.

This document is intended for general purposes only and should not be construed as legal or coverage advice on any specific matter.

RECOGNIZING PHISHING SCAMS

- The sender's address is in a different format than the rest of the organization's (e.g., all e-mails within the organization follow the format of "firstname.lastname@co.county.mn.us" but the message claiming to be from someone within the organization is different).
- There are frequent misspellings and poor grammar. Many attacks originate in non-English speaking parts of the world.
- The message asks users to click on links or open attachments.
- If anything sounds too good or too bad to be true (e.g., "Claim your tax return now" or "We have your kids.")
- The message includes outrageous or sensational headlines or imagery that entices you to click on them.
- The message is in a spam or junk e-mail folder. Many IT departments and e-mail providers have filters that automatically screen spam messages. If a message is in the spam folder, it can be a clue that it may not be legitimate.
- There is a vague greeting and sender. Often bulk phishing attempts are not directed to individual people. Messages may start with "attention" or another generic word or phrase. Similarly, messages that end with a title or vague location should be viewed with suspicion (e.g., "web administrator or "help desk").
- Hovering the mouse cursor over the link shows a different Web address than the indicated link.

PREVENTION

If a message has one or more of the elements above, you should:

- Contact IT.
- Follow IT directions.
- Do not open the message, click on any links or items or follow instructions in the message, such as sending confidential information or passwords.
- Forward any requests for private information to the responsible authority for your organization.

This document is intended for general purposes only and should not be construed as legal or coverage advice on any specific matter.