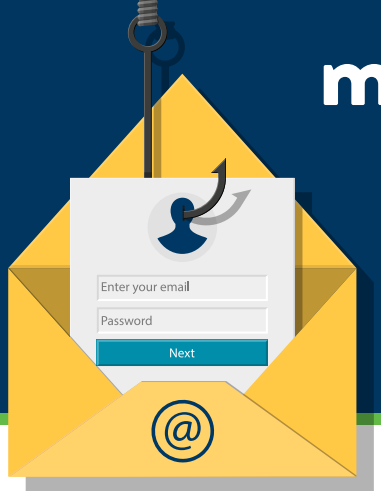
PHISHING ATTACK PREVENTION

Email action steps

MINNESOTA IT SERVICES



Stop and question it

- Pause and take a minute to review the content.
- Identify whether the message is from a known or trusted source.

Examine it

- Hover the cursor over the sender address, link, and/or attachment to ensure they are valid.
- Look through the email for potential attack strategies in use.

Don't respond

- Don't click on links, open attachments, or provide any information.
- Never provide passwords, sensitive information, or financial data.

Make contact

- Use legitimate contact information to confirm directly with the source that the message is valid.
- Check known news and government sites for information and confirmation.
- Set up safe words with family and friends to verify each other's identity.

Report it

Suspicious email

- Report suspicious emails to the email platform. Many, including Gmail, Outlook, and Mac Mail, have phishing report features.

Security incident

- Contact the Federal Trade Commission at ftc.gov for security incident and identity theft resources.