FACT SHEET

Helpful Hints to Avoid

PHISHING SCAMS

& PROTECT YOURSELF AND YOUR BUSINESS.

What is a phishing email? How could it affect you or your business?

This 5-billion-dollar industry is the fraudulent practice of sending emails that are pretending to be from reputable companies to tempt people to reveal personal information, such as passwords, credit card numbers, or to infect the user with malware by having the user click an infected link or attachment.

What are malware and ransomware?

Malware is malicious software that's intended to steal information, or damage/disable computers and computer systems. Ransomware is an increasingly popular type of malicious software that denies access to a device or files by encrypting/locking them until a ransom has been paid. This can be triggered by opening a bad attachment, or by visiting an infected link.

What you can do:

- Always remember to hover your cursor over a hyperlink to view the URL and determine if the website makes sense.
- Ask yourself: Is the email expected? Do you recognize the person or company that sent you the email? If not, it may be best to delete it.
- Does the grammar and spelling look appropriate? Many phishing emails come from other countries.
- Is the email demanding your attention, or urging you to do something immediately, such as, "your account will be closed if you do not respond"? These types of scare tactics are generally indicators that the email is fraudulent.

Think before you click.

Gorham SAVINGS BANK

Banking is believing℠