What is Phishing?

Phishing is a scam that usually involves email messages that are designed to appear from a trusted source. The objective of these emails are to persuade you into providing sensitive information.

By replying to and providing personal information to these emails, phishers can use this information to gain access to your sensitive data and possibly steal your identity. This can include:

- Bank accounts
- Social Media accounts
- Medical records
- Email accounts
- Gettysburg College account

The following items should **NEVER** be shared through email:

- Social Security numbers
- Passwords
- Credit Card numbers
- Bank Account numbers
- Driver's license numbers
- Names, addresses, and phone numbers in conjunction with other personal data
- Health, financial and student educational record information

Spotting a Phish

Phishing Emails tend to contain the following suspicious attributes:

- Creates a sense of urgency and impending deadline
- Use of Poor Spelling and Grammar
- A forged sender's address
- A Generic Greeting
- Fake web links
- Login links
- Attachments from Businesses
- Fear of losing money or important information
- Files that require you to download additional software
- The website URL doesn't match the name of the institution it represents.

When Receiving Emails

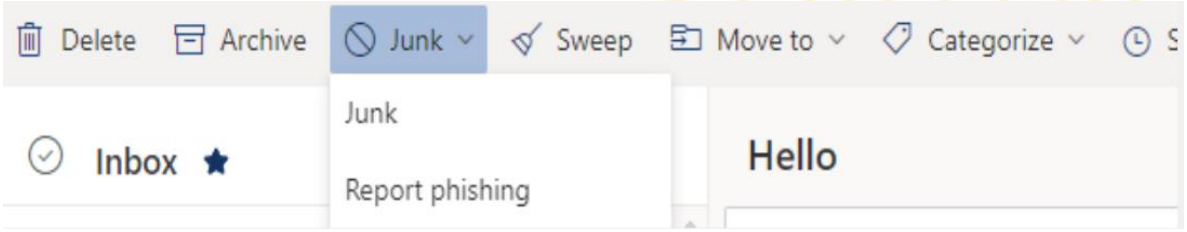
With every email you receive, you should always ask yourself questions similar to the following before doing anything else:

- Do I know this sender?
- Does this email contain common phishing attributes?
- Have I ever received an email from this person or company before?
- Why are they sending me this email?
- Was I expecting this email?
- Does this email seem legitimate or realistic?
- Why are they asking for certain personal information?
- Does this email make me feel anxious and reactive?

Stranger Danger!!!

You received a Phishing Email but didn't click on anything, now what?

- If you're a student and received a phishing email, you can report the message as phishing. There is a Report Phishing feature built-in to Outlook Office 365. It is located under the **Junk** tab. If you have trouble finding the tab, you can just delete the message. Students are also asked to forward the message as an attachment to phishing@gettysburg.edu.



- Employees using Outlook or OWA can mark the message as Junk or delete the message after reporting the message to phishing@gettysuburg.edu
- If you're unsure that what you received is a phishing email, you can take a screen shot of the email or simply forward the message as an attachment to phishing@gettysburg.edu or to the Gettysburg College ITHelpdesk, trouble@gettysburg.edu. Don't hesitate to email or call the Helpdesk at 717.337.7000 to be advised on the best course of action.

You received a Phishing email and fell for it (either by clicking a link or replying to the sender), now what?

- Assume the worst. Depending on what information you may have supplied, **immediately change your Gettysburg College Network Password**. If the same password is being used in multiple locations for other accounts (you shouldn't do this!) it would be wise to change the password for those accounts as well.
- If you need further assistance, call the Gettysburg College Helpdesk at 717.337.7000 or email trouble@gettysburg.edu

Rule of Thumb:

- Click Carefully! When in doubt, reach out.

******* Gettysburg College will NEVER send you an email asking for your Password*******