Phishing Emails

What is Phishing?

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Many websites have now created secondary tools for applications, like maps for games, but they should be clearly marked as to who wrote them, and you should not use the same passwords anywhere on the internet.

Tips to Identify Phishing Emails

- Most phishing campaigns want your username and password to be entered into some external website.
- Most phishing emails express urgency and threaten penalties. For example, "Click this link and provide your id and password. Failure to do so within 24 hours will cause your account to be suspended!" ITS will **NOT** send these types of messages.
- Most phishing emails are very generic. They lack individual signage, phone numbers, institutional graphics, and distinct contact information.
- Most phishing messages pretend to be from someone you know internally but in actuality come from outside of our network. For users with @fairfield.edu emails, if the [External] tag exists on the subject line, the message is from someone outside our organization.
- Most links within a phishing email will really point towards odd external websites. Hover over any email links before clicking. Make sure the website URL makes sense for the request.
- Most phishing emails contain incorrect spelling and odd grammar. Occasionally this is intentional to avoid phishing filters.
- Some phishing emails are completely unique, don't follow any of these rules and appear completely legitimate. It's important to maintain a healthy skepticism when it comes to your email. If you are ever in doubt forward the message in question to phishing@fairfield.edu. We can examine the message on your behalf.

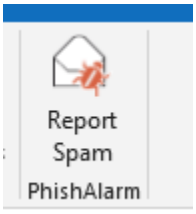
Why was the phishing email not blocked?

Fairfield University has a variety of safeguards in place combating known viruses and phishing attempts. Millions of threating emails are stopped before any University employee or student sees them, by design. On occasion, an email will slip through the safeguards. If you receive what you suspect to be a dangerous email, **delete it**. Cyber security starts with users being informed and continually looking out for anything that seems suspicious.

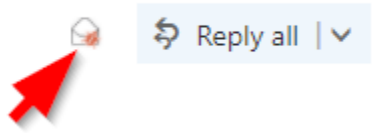
I think an email I received might be phishing

Use the Report Spam button in Outlook or Outlook Web Access to report the email. This will start an automatic analysis of the email and will delete the email from your inbox.

Outlook:



Outlook Web App:



If this fails to work or you can't find the button please forward the email to phishing@fairfield.edu. Please include the header information if possible as this will help us identify where the email was coming from and stop others from receiving it. To obtain the Internet Header, see instructions below:

For OWA: Double-click the message to open it, and then click the Message Details icon (an envelope with a small document over it).
For Outlook on Windows: Double-click the message to open it in a new window. Select the File tab, and then click Properties.
For Outlook on Mac: In your Inbox (or other folder), right-click or `control`-click the message, and then select View Source.

After you forward the email to phishing@fairfield.edu, please delete the email and delete it from your deleted items folder as well.

Please do remember that ITS employees will NEVER ask you to provide your NetID password. Users should never willingly share their passwords with anyone, either via e-mail or website other than the official Fairfield University website. Should you receive any requests via e-mail asking for your NetID credentials, do not respond to the e-mail, do not open any associated attachments or visit websites referenced within it.

For further assistance, please visit the ITS Help Desk located in NYS 215 or call 203-254-4069 during business hours.

Hours can be found here: ITS Help Desk Hours of Operation