Phishing Emails

Phishing Emails

REPORT phishing messages to the ITSservicecenter@fredonia.edu then DELETE them.

If you responded to a phishing message, contact the ITS Service Center immediately at ITSservicecenter@fredonia.edu or 673-3407.

Verify an Official Fredonia Email

If you received an email and you are unsure if it is a legitimate message, forward the message to ITSservicecenter@fredonia.edu. Fredonia ITS staff will verify whether or not it is legitimate.

What is a phishing email?

- Phishing emails are messages sent by individuals trying to "fish" for personal or financial information. Phishers are getting better every day at making their messages look authentic. There are two types of phishing emails:
- Emails that ask you to reply to the message with confidential information, such as your user ID and password. Never respond to any email with confidential information. Fredonia and other legitimate businesses will never ask for this information via email.
- Emails that ask you to click on a link to a webpage, which then asks you to provide confidential information. Many times these webpages look like legitimate sites, such as Bank of America or PayPal, but they are not. When you provide your user ID and password, this information is captured by the phisher, who can then use it to log into the legitimate site.

What to do if you get a phishing email

Send any phishing emails you receive, including its full header information, to ITSservicecenter@fredonia.edu.

- If you suspect it may be a phishing email, Fredonia ITS can review the message and advise if it is legitimate or not.
- If you know it is a phishing email, Fredonia ITS can take measures to have the phishing website taken down.
- Never respond to any email with confidential information. Fredonia and other legitimate businesses will never ask for this information via email.
- Use your mouse to hover over links in an email. This will show you the actual website you will be directed to if you click on the link. It is always best to type the address yourself into your web browser, rather than clicking a link in an email.

Phishing emails:

- May show the sender on behalf of someone, such as the Fredonia, and generally does not contain the sender's email
- May contain fuzzy logo symbols, which are not genuine
- May not contain email signatures or any contact information
- May contain bad grammar and capitalization errors
- Generally require you to take quick action, such as verifying your account to prevent it from being deactivated
- Be particularly vigilant during holidays or during significant events since attackers heighten their activity during these times.

How to Protect Yourself

- Here are some best practices that will help protect you and your information:
- Beware of messages that claim your account has been suspended
- Be suspicious of any email containing urgent requests for personal financial information
- Never click on a link in an email. Instead, always type the legitimate Web address of the site you want to reach directly into your Web browser.
- Be suspicious of email messages and other electronic communications from sources you do not know or recognize
- Use the latest versions of your operating system (OS) and applications
- Have the latest security software updates (patches) installed. This includes patches for your OS and applications
- Keep your anti-virus software up to date
- Report any suspicious emails

Short URL to this page: https://answers.fredonia.edu/x/$action.getTinyUrl()

Related articles

- Virtru Protected Email Guide
- Fredonia Mail Data Loss Prevention Policy for Credit Card Numbers (CCN) and Social Security Numbers (SSN)
- How do I mark or unmark Spam in Gmail?
- How do I setup FREDmail for mobile?
- How do I login to FREDmail for the first time?