UNIVERSITY OF HARTFORD
DEPARTMENT OF PUBLIC SAFETY

Routine: (860) 768-7985
EMERGENCY: (860) 768-7777
Anonymous Tip Line: (860) 768-**7827**

Important information about phishing emails and protecting yourself.

Something's phishy if

- The content presents a false sense of urgency. Look out for statements like "failure to take immediate action will lead to your account being permanently deleted!" Or the sender is posing as a family member, friend, classmate or coworker asking for money, gift cards or electronic currency.
- The email, text, or voicemail is requesting that you update/fill in personal information. Treat any communication Asks for passwords, bank account information, usernames, credit card numbers, social security numbers, etc use extreme caution.
- Displays fake URLs that actually direct you to dangerous sites. The URL shown on the email and the URL that displays when you hover over the link are different from one another.
- The "From" address is an imitation of a legitimate address, especially from a business or co-worker.
- The formatting and design are different from what you usually receive from an organization. This could be something like the logo looking pixelated or the buttons having different colors. There could also be weird paragraph breaks or extra spaces between words. If the email appears sloppy, start making the squinty "this looks suspect" face.
- The content is badly written. Sure, there are plenty of wannabe writers working for legitimate organizations, but this email might seem particularly amateur. Are there obvious grammar errors? Is there awkward sentence structure, like perhaps it was written by a computer program? Take a closer look.
- The email contains attachments from unknown sources that you were not expecting. Don't open them, plain and simple. They might contain malware that could infect your system.

If You Are Compromised

- If you believe you might have inadvertently revealed sensitive university information such as your NetID password, you should change your password immediately. If you have questions, or concerns contact the Office of Technology Services at helpdesk@hartford.edu or 860.768.4357.
- If you provided personal information that could be used for identity theft or fraud in response to a fraudulent email, you should immediately contact the bank, creditor or company being spoofed. To make a report on campus or for help documenting possibly having been compromised you can contact The Department of Public Safety at 860.768.7985

Report Phishing

Please report suspicious emails to the help desk by forwarding them to helpdesk@hartford.edu or by calling 860.768.4357.

SEE SOMETHING – SAY SOMETHING
Safety on Campus
A Shared Responsibility