

Phishing Email

What is phishing?

Phishing is a common email-based attack used by cyber criminals to steal information from you. A phishing email pretends to be from someone or something you know or trust, such as your bank or your favorite online store, then tries to entice you into taking an action, such as clicking on a link, opening an attachment, or responding to a message. The goal is to fool you into providing personal and confidential information, such as logins, passwords, bank account or credit card numbers, or your mother's maiden name. Phishing emails and websites may look legitimate with exactly the same look and feel of your online bank or retailer, but they are designed to steal information that could give them access to your online account. Cyber criminals craft these convincing emails and send them out to thousands, if not millions, of people around the world. The criminals do not have a specific target in mind, nor do they know exactly who will fall victim. They simply know that the more emails they send out, the more people they may be able to fool.

Reporting phishing attempts

If the message contains an address (URL) for a phishing site, report the site using either

- Google's Safe Browsing utility, found at google.com/safebrowsing/report_phish/
- Phish Tank, found at <http://www.phishtank.org>

If you receive an email that you suspect is a phishing attempt in your @case.edu email account, and it appears to come from a cwru.edu or case.edu email address, please forward the suspicious message to help@case.edu

To remove suspicious email from your CWRU Google email (webmail) inbox, select the message and click the **Report Spam** button. All future messages from the address will be labeled as Spam.

More information on understanding, detecting, and reporting phishing can be found at securingthehuman.org/newsletters/ouch/issues/OUCH-201112_en.pdf

How phishing works: <http://preview.tinyurl.com/853xj85>