Phishing 101

What is Phishing?

Phishing refers to online fraud, in which you are tricked into revealing personal information for the purpose of identity theft (email account details, banking information, etc.). These impostors operate by impersonating businesses. The number one rule with phishing is to NEVER reply to email, text, or pop-up messages that ask for your personal or financial information. CSULB and other legitimate businesses do not ask you to send such sensitive information through these unsecure methods.

What is Spear Phishing?

Spear phishing is an email-spoofing attempt that targets a specific organization or individual. It often seeks unauthorized access to sensitive information. They are known to be attempts by perpetrators that are out for financial gain, trade secrets, military information, or intellectual property. Often times, the sender masquerades (spoofs) as someone that is known by the email recipient.

What is the University Doing about Phishing?

The university's email system currently intercepts thousands of malicious email per year (spamming and phishing). Unfortunately no email system provides 100% protection, so some of the university's email system defenses rely on you – the email user.
As an extra measure, as soon as ITS is alerted of any new phishing attempts targeting campus employees, links that are included in the phishing emails are blocked so that if any on-campus users attempt to click on the link, it will not work. The block, however, does not work if the phishing link is accessed when you're off campus.

How to Determine if an Email is a Phishing Attempt

If a message asks you to email your password or account details it is almost definitely a phishing email or from a website that is likely to be a fraud. CSULB will never ask you to email your password or account details. Other clues:

- The "from" address and/or the "reply-to" address are not from legitimate campus sources (gmail.com, google docs, yahoo.com, etc.)
- The message warns of a big change but has no email address or phone number for further information.
- The message has poor spelling and grammar
- The message carries a threatening tone, a sense of urgency, and/or warning if you do not comply
- It has a non-standard salutation such as "**Dear account user**" or "**Dear valued customer**"
- It uses a lot of capital letters, e.g. "**Dear WEBMAIL ACCOUNT USER**"

View some Examples of Phishing Messages.

View a printable poster from the SANS Institute

Click on image below to open:

View the latest phishing attempts targeting campus employees.

How do we respond to phishing attempts? See ITS Phishing Alert Process.

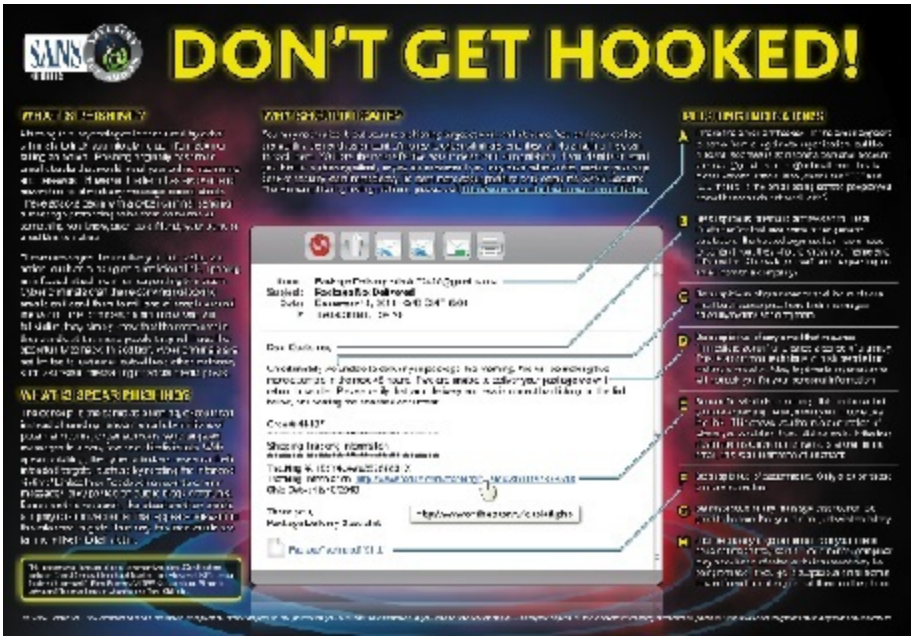

Figure 1: Don't Get Hooked poster

How to Handle Phishing Emails

- Never reply to an unsolicited email that asks for your personal information. CSULB will never request personal information asking you to such info by email (i.e., your Campus ID, SSN, email password, birth date, or any account numbers). Other reputable institutions (your bank, credit card company, or loan officers) would not email you requesting you send this type of information by email either.
- Never click on any links within a suspicious email. Links within a phishing email often lead to fake internet sites. For example, a phishing email may contain the link "Click here to update your information" and then lead to a phony business website requesting personal information. Always visit an institution's website directly, using their official URL (website address). When in doubt, you may contact your campus technical coordinator to verify if an email is from a credible source.
- Label the message as junk. For instructions on how to do this, visit the IT Knowledge Base (https://its-knowledge01.campus.ad.csulb.edu/x/I4AQAQ). Then go to your junk folder to delete the email. By labeling it as junk, it prevents you from receiving email from the sender again.
- If you're concerned about your account or need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card.
- Always use common sense and good judgment. The university operates a broad array of security-related hardware and software designed to safeguard sensitive personal and institutional data. However, our networks and services are connected to the Internet, and we cannot block every fraudulent action that occurs on the world wide web. We need everyone to look carefully at what appears in your email - if it looks suspect, it probably is.

Action Steps If You Fall Victim to a Phishing Scam

If you responded to a phishing attempt while using university email:

- As a precaution you should change your password immediately by visiting BeachID Accou nt Manager. You may also contact your campus technical coordinator for any additional instructions if necessary.
- Contact the organizations where the information could potentially be used. For example, if you provided a username and password for your bank to a phishing site, contact your bank. If you provided your personal information, like your social security number, contact the credit bureaus. In some cases you may need to file a police report and contact the Federal Trade Commission (FTC) at www.ftc.gov/complaint. Visit the FTC's Identity Theft website; victims of phishing could become victims of identity theft; there are steps you can take to minimize your risk.

Report Phishing Emails

Forward phishing emails to alert@csulb.edu. Depending on the nature of the phishing email, you may also want to forward the email to the company, bank, or organization impersonated in the email. You also may report phishing email to **reportphishing@antiphishing.org**. The Anti-Phishing Working Group, a group of Internet Service Providers, security vendors, financial institutions and law enforcement agencies, uses these reports to fight phishing.

Many Phishing attempts utilize Google Docs as a webform for users to enter their personal information. To report abuse of Google Docs to Google, follow their procedure: https://support.google.com/drive/contact/drive_abuse.

Return to All Phishing Reports.