“Phishing” emails appear to be from a legitimate source but trick you into providing personal information or credentials.

Please forward all suspicious messages to abuse@ucdavis.edu.

Only seek IT technical support from 1-916-734-HELP.

Learn more: https://health.ucdavis.edu/itsecurity/

How to Spot Phishing Messages Like a Pro

The Federal Trade Commission defines phishing as “when a scammer uses fraudulent emails or texts, or copycat websites, to get you to share valuable personal information.”

https://www.consumer.ftc.gov/articles/0003-phishing

While we rely on security technology to minimize threats, phishing uses social engineering to take advantage of us, which can allow malicious cyber criminals to sidestep protections.

This is why it is important for everyone learn to spot these fraudulent messages. Think you’ve got a good eye for an attempt to phish your personal information?

Let’s take a look at some example phishing email messages.
Message #1
Subject: Low Cost Dream Vacation loans!!!

Dear John,

We understand that money can be tight and you may not to be able to afford to go on vacation this year. However, we have a solutions. My company, World Bank and Trust is willing to offer low cost loans to get your through the vacation season. Interest rates are as low at 3% for 2 years. If you are interested in getting a loan, please fill out the attached contact form and send it back to us. We contact you within 2 days to arrange a deposit into your checking account.

Please email your completed form to VacationLoans@worldbankandtrust.com.

Your dream vacation is just a few clicks away!

Dr. Stephen Strange
World Bank and Trust
177a Bleecker Street, New York, NY10012

What do you notice in Message #1?
The phisher wants to give you a low cost loan with no credit check. They say that you just need to send them your information and they will give you money, right? Not only does it seem too good to be true but, if you are looking at this on a computer, hover the cursor over the email address and examine it closely. You will see that the link actually has a different destination. It is the email address of the attacker. In addition, there are spelling and grammatical errors. Whatever you do, don’t open the attachment! It could be riddled with malware and viruses!

Message #2
Subject: Free Amazon Gift Card!!!

Dear Sally,

You name has been randomly selected to win a $1000 Amazon gift card. In order to collect you prize, you need to log in with your Amazon account at the link below and update your contact information so we can put your prize in the mail. This is a limited time offer, so please respond to the request within 2 business days. Failure to respond will forfeit your prize and we will select another winner.

www.amozan.com/giftredemption2321

What do you notice in Message #2?
It’s too good to be true. “Amazon” is misspelled as “Amozan” on the link. If you respond, you will be providing your information to an attacker. Again, if you’re looking at this on a computer, hover over the URL. For the purposes of this example, the link actually navigates to the Center for Internet Security, which is a trustworthy site.

Message #3
Subject: Urgent – Take Action Before Your Email Account is Deactivated

Dear User,

Following changes to our Microsoft email systems, each user must authenticate their account to prevent it from being deactivated. You can accomplish this by heading to the link below and entering your Microsoft Outlook email account credentials, and then we will know your account is active and should remain so.

http://www.microsoft.com/

Thank you,
Information Technology
Helpdesk Support Team

What do you notice in Message #3?
This email is fairly well-crafted without spelling or grammatical errors. Note that it establishes a sense of urgency that the malicious cyber criminal hopes will cloud your judgement and threatens the deactivation of your email account. Additionally, the link at the bottom looks like a link to Microsoft, yet it is in fact heading somewhere else! Luckily, for the purposes of this example, that link simply leads to the Center for Internet Security, which is a legitimate site.