HELP PROTECT YOURSELF AND CUESTA: HOW TO IDENTIFY PHISHING SCAMS

DECEPTIVE PHISHING

Email messages claiming to come from recognized sources asking you for account information or to make a payment.

SCAM OBJECTIVE: To trick you into providing the details needed to access your accounts.

HOW TO AVOID IT: *Look out for generic greetings and/or requests for information that the sender should already have. Check the date/time – if it was sent at an unusual time, it could be a sign of a phishing attempt.*

SPEAR PHISHING

A more sophisticated version in which the sender uses available information to direct their request at you.

SCAM OBJECTIVE: Directly target you to acquire account/banking details.

HOW TO AVOID IT: *Look out for typos, and alarming threats or ultimatums. Be cautious when the email is coming from someone you have had no past communication with.*

AUTHORITY FRAUD

Phishers use an email address similar to that of an authority figure to request payments or data from other employees in the college.

SCAM OBJECTIVE: For the victim to transfer money/confidential information directly to the cybercriminals.

HOW TO AVOID IT: *Anytime you receive an email that is unusual or out of character double-check suspicious requests with the sender before sending sensitive information that would put the business/individual in jeopardy, by phone or in a separate email.*

PHARMING

Fraudsters hijack a website's domain name and use it to redirect visitors to an imposter site.

SCAM OBJECTIVE: To intercept and steal online payments.

HOW TO AVOID IT: *Check to confirm that the URL ,of the site that is asking for data, is authentic. If you cannot determine the trustworthiness of the URL , forward the email to IT for support.*

DROPBOX PHISHING

Realistic-looking emails claiming to come from Dropbox request, asking the user to click through to "secure" their account or download a shared document.

SCAM OBJECTIVE: To install malware on the victim's computer.

HOW TO AVOID IT: *Ask yourself – "Is this an unexpected, illogical or odd email with an embedded link or attachment." If it your gut feeling tells you the request is unusual, don't follow the directions of the sender.*

GOOGLE DOCS PHISHING

A message invites victims to view documents on Google Docs. The landing page is indeed on Google Drive so it seems convincing, but entering your credentials will send them straight to the scammers.

SCAM OBJECTIVE: Access to your Google account, including Gmail, Google Play and Android applications.

HOW TO AVOID IT: *Examine the page carefully for errors, such as corrupt characters in the language selection box. Check which service you are entering – it is listed below "One account. All of Google"*

If you feel you may be a victim of a phishing scam, forward the email to UserSupport@cuesta.edu