Phishing & Spam Awareness

Computer Services has addressed the problem of phishing attacks and spam using various communiqués and training vehicles promoting awareness at Cuesta College:

- Regular e-mail alerts and reminders (pages 2-6)
- Classes on “Safe Computing” (*dropped a couple of years ago due to poor attendance*)
- Numerous postings in the “T3...” channel’s “Tip of the Week” section (*pages 7-9*)

Computer Services continues to explore creative and effective ways to heighten awareness and eliminate unauthorized e-access.
Examples of E-mail Alerts and Reminders

From: "Cuesta College Computer Services" <cecs@cuesta.edu>
To: "All Exchange Users Email List" <ALL@cuesta.edu>
Cc: 
Date: Mon, 25 Oct 2010 11:27:54 -0700
Subject: No Joke - Please Read

Riddle of the Day

**QUESTION:**
What did the wise computer-user do after receiving an e-mail request for their password?

**ANSWER:**

Nothing!

It’s no joke.

NEVER, NEVER, NEVER give out your password (or other private information) via e-mail. If you receive a suspicious e-mail requesting personal data and you’re unsure as to what to do, contact Computer Services (x3248 or 546-3248).

Be smart! Don’t fall victim to a phishing attempt.

Let yours be the last laugh!

For more information, check out:
http://www.cuesta.edu/deptinfo/elic/training_materials/War.pdf
Phishing attempts continue to sneak into Cuesta employees’ e-mailboxes. Don’t be fooled!

- Always check e-mail From addresses. If it’s not a “...cuesta.edu” address, beware!

- If you’re not sure of the e-mail’s sender, **never** click on an embedded link ← like this one.

- If you’re not sure of the e-mail’s sender, **never** open an attachment.

- **NEVER** give your password (or other private information) to anyone via e-mail!

If you have any questions, please call Computer Services (x3248).
BEWARE! Despite our best efforts, some phishing e-mail and spam continue to sneak into Cuesta employees’ Inboxes.

This means you need to be on your guard when it comes to e-mail, ready to distinguish the bogus from the bona fide.

So, can you can spot the identifying characteristics of this latest phishing attempt!

Click here if you would like to verify your answers.

And remember, if you have any questions about e-mail contact Computer Services (x3248).
Just a reminder that phony e-mail continues to sneak into Cuesta College. These bogus communiqués try to lure you into revealing your password and other private information. Please don’t fall for these “phishing” attempts!

- **Check the author’s** (FROM) address!
  
  Is it from Cuesta College (i.e. “…cuesta.edu”)?

- **Check the text.**
  
  Does it even mention “Cuesta” or “Computer Services”?

- **Check embedded links.** (NEVER click on the link in questionable e-mail! Point at the link to view its destination.)
  
  Does it go to a “…cuesta.edu” site?

- Remember, **never give your password** or other personal information over e-mail.
  
  *Computer Services will never ask for your password via e-mail.*

When in doubt, call or e-mail Computer Services.

Thanks for being smart and careful.

---

Below is an example of a recent phishing attempt. The hyperlink (which pointed to Germany) has been removed.

```
From: p.buchta@ieee.org [mailto:p.buchta@ieee.org]
Sent: Tuesday, January 24, 2012 8:45 AM
To: undisclosed-recipients
Subject: Notice! Notice!! Notice!!!

Your Mailbox Has Exceeded It Storage Limit As Set By Your Administrator, And You Will Not Be Able To Receive New Mails Until You Re-Validate It. To Re-Validate -> Click Here: System Administrators
```
Examples of Tips of the Week

The “T3 – Tech Tips & Training” channel in myCuesta features a “Tip of the Week” section (see below), which often contains phishing and spam tips.

Previous tips are accessible via the “Tip of the Week Archives” link, also in the “T3...” channel. (NOTE: The archives URL is http://academic.cuesta.edu/training/mycuesta_tipoftheweek_archive.htm)

The following are examples of past spam and phishing tips taken from the Tip of the Week Archives:

---

It's Phishing Season! Beware Unusual E-mail!
July 10, 2012

Received any e-mail from "Cuesta" requesting your password or offering to fix a problem?
Don't fall victim to a phishing attempt. Test that dubious e-mail using this Phishing Check List!
When in doubt contact Computer Services (x3248).
Malware Increases on PCs, Macs and Smart Phones!

May 24, 2012

McAfee reports an increase of malicious software on all platforms. Click here for article and report. Protect yourself by (1) updating & securing your computer, (2) being skeptical of pop-ups, error messages and attachments, (3) removing spam, (4) reconsidering new software, and (5) using common sense. Get more info here, and here (for Mac-users), and here.

Be On Your Guard Online. Check Out "OGOL"

May 11, 2012

Avoid scams. Secure your computer. Protect your kids online. This and much more is available at OnGuardOnline.gov. Click here to check out the site.

Phishing Alert from Verizon

April 9, 2012

Verizon Wireless is warning customers of phishing attempts disguised as payment confirmation. Click here to view Verizon's warning (to PG&E)

Mac Malware Alert!

March 7, 2012

Mac users beware! Intego reports a new variant of the Flashback Trojan. Click here for more info.

Tax Season Phishing Scams and more!

February 9, 2012

The US Computer Emergency Readiness Team is reminding users to remain cautious of potential tax-related phishing scams or malware campaigns. Click here to read the US-CERT's warning.

iPhone bug enables FaceTime, shows names on locked phones

Attention iPhone users: Apple's security measures to keep people from viewing your contacts and instigating FaceTime video chats may not be so secure. Click to read C/Net article.
Beware Smishing!
February 1, 2012

"I just got a text message from Yahoo saying my account has changed and I need to go to a web link to fix. Oh, wait...I don't have a Yahoo account!"

Yes, it's not just phishing e-mail you need to be on the lookout for. "Smishing" (text-to-phone phishing) continues to be a problem. Be smart; don't just respond to text messages. Beware and be safe. Click here for more info on smishing.

Beware Fake MS Tech Support!
Last week CalPoly issued a campus-wide warning re: bogus Microsoft support calls. If you receive such a call, please inform Computer Services (x3248). Click here for details.

What's Your Phishing IQ?
November 11, 2010

Think you're pretty smart, huh? Well, prove it by acing this short phishing quiz. And just to sweeten the incentive, we're giving away chocolate to four (4) lucky test takers!

Click here to take the quiz. Once completed, print the results page and sent it (interoffice) to "TechTrainer, Computer Services". Regardless of your score, you'll be entered in a drawing for some yummy, exotic chocolate!