Information Security Bulletin

Issue #2012-02

Raising awareness of information security related issues and concerns.

Common Scams

E-mail requesting you verify your account info. This common scam often looks like it comes from a trusted source such as the college’s webmaster or service desk, a bank or other financial institution, credit cards, etc. They almost always include links and requests for passwords along with the account name. There are often misspellings or unusual grammar in the e-mail although many scammers have started learning the value of spell check. No reputable organization needs you to send them your password. Please be aware that the e-mail’s From line can be spoofed and you cannot rely on its accuracy. If you receive one of these in your college account and have seen others like it, just delete it. If you haven’t seen a similar one before, please forward a copy of the e-mail immediately to any member of the Information Security Team. Be sure to use the “Attach Item” function in Outlook (call x6440 if you need help doing this). If you responded and gave them your credentials, please call the Information Security team for help. For all non-EPCC accounts, click delete.

E-mail that you won/inherited money or someone needs help getting their inheritance out of a foreign country. Not a week goes by that someone at EPCC gets one or more of these. Usually in an e-mail, this has numerous variations. One variation is that you are a long lost relative of a rich person and have inherited gazillions. Another common variation is that you won a lottery that you didn’t even enter. A third common variation is a widow needs help. They promise that all you need to do is cooperate by sending the taxes and/or other fees to the administrator or lawyer handling the case. If you respond, what will happen is you will send more and more money to the scammer and nothing will happen beyond the loss of your money. If you receive one of these, click delete and smile because you were too wise to be fooled.

Free IPAD for testers One of Facebook’s most enduring and prevalent scams mainly exists because curious people click to check it out. Clicking will almost certainly cause you a great deal of embarrassment as the script on the page changes your facebook settings and sends a similar message from you to everyone on your friends list. This particular scam not only embarrasses you on facebook but often results in downloads of malware to infect your computer. When you see these posts, please use Facebook’s link for reporting spam (usually in the upper right corner) so the Facebook staff can deal with it appropriately. If you suspect you infected a college computer, please call x6440 to initiate a work order so the technician can clean it up at no charge to you. Leaving the malware on the computer could cause harm to any co-worker who uses that machine.

IRS & Tax related emails. Every year at tax time, there is a definite increase of e-mails, fax or phone messages from creative scammers that claim to be from the IRS or concern refunds. If you receive these kinds of e-mails, please forward the e-mail to phishing@irs.gov.

Illegal Debt Collection. There has been a large increase in deceptive, abusive debt collectors and the Federal Trade Commission has brought several to justice in the last year. These illegal behaviors include misrepresentations to collect on debts that they in fact weren’t authorized to collect on, or that consumers did not owe; relentlessly calling the victim’s home, cell phone, and place of employment in attempts to obtain payment; threatening physical harm to the individual, their loved ones and their pets; impersonating process servers, attorneys, FBI agents, and other officials, falsely threatening to sue and arrest those whom they claimed owed money, etc. If you are being targeted whether or not you legitimately owe the debt, we recommend you take the time to read the FTC’s Debt Collection FAQs: A Guide for Consumers found at http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre18.shtm. If you are threatened, call the police department immediately. File complaints at the Internet Crime Complaint Center in English or Spanish at http://www.ic3.gov/.

For further reading, we recommend:

- Phishing and other schemes using the IRS name http://www.irs.gov/newsroom/article/0,,id=214917,00.html
- Common Online Scams http://onguardonline.gov/articles/0002-common-online-scams
- 16 Ways You Can be Phone Scammed http://800notes.com/arts/LFRVNXyqwQBxqRajLF8wQyg

Information Security Team:

Cheryl Bowman, Information Security Risk Advisor 831-6574 cbowman@epcc.edu
Richard Becker, Security Analyst 831-6411 rbecker3@epcc.edu
Richard Buller, Chief Information Security Officer 831-6312 rbuller@epcc.edu

El Paso County Community College District does not discriminate on the basis of race, color, national origin, religion, gender, age or disability.