Current Scams - January, 2013

Scams are ever changing and here are ones that appear to be making the rounds lately:

**Strange Skype calls.** This scam starts with a stranger’s call from an unfamiliar phone number such as 661-748-0240 (Skype’s default number) or other spoofed numbers. The caller requests a specific individual by name. Once that individual answers the call, the caller immediately begins asking personal questions. It is perfectly fine to hang up on these individuals, they are almost always phishing for answers to your security questions. Please keep in mind, EPCC operators do not screen your calls and will put through all calls asking for an employee by name. At EPCC, if the caller makes you uncomfortable by asking personal information, write down the phone number and pertinent information, hang up and then call the the Information Security Program at x6480 or the EPCC Police Department at x2200. If you are at home when you receive the call, contact the local Police Department to make a report and then file a complaint with the FTC at http://www.ftc.gov.

**You Violated Federal Law!** This scam starts with a popup on your screen and pretends to be from the FBI, the ICC or similar government agencies. It threatens prosecution on child pornography related charges unless the individual pays a fine using prepaid money card services. The software often locks the computer. Please note: even if you are successful at unlocking the computer, malware can continue to operate on the compromised computer to commit online banking and credit card fraud. Read more at http://www.epcc.edu/IT/InformationSecurity/Bulletin_Archives/Infosec%202012-08.pdf

**Emergency! I Need Money!** This has been a highly successful scam, preying on our natural desire to help a friend or loved one. It invariably involves someone stuck somewhere with lost wallets, passports or who had an accident and is in jail. They invariably require you to wire money using Western Union or another transfer service. The El Paso Times recently had an article where a loving grandmother almost fell victim to sending $2,800 to someone masquerading as her grandson and claiming he was in jail in Peru due to an accident. Before she released the confirmation number for the Moneygram, she fortunately decided to call her grandson to let him know money was on the way only to discover he wasn’t even in Peru. Read more about the Peru case in the El Paso Times at http://www.elpasotimes.com/ci_22449444.

For further reading, we recommend:

- Phishing and other schemes using the IRS name http://www.irs.gov/uac/Report-Phishing
- Snopes top 25 hottest urban legends http://snopes.com/info/top25uls.asp
- Common Online Scams http://onguardonline.gov/articles/0002-common-online-scams
- 16 Ways You Can be Phone Scammed http://800notes.com/arts/LFRVNXyqwQBNrAjLF8wQyg

Information Security Team:

**Cheryl Bowman,** Information Security Risk Advisor 831-6574 cbowman@epcc.edu

**Richard Becker,** Chief Information Security Officer 831-6411 rbecker3@epcc.edu

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