



Monthly E.C.C. Staff Information Security Briefing

Date: 11/28/2016

This is the first in a monthly series of information security briefings that are intended to raise the cyber awareness of all E.C.C. Staff. Each month there will be a new tip or training segment that will help educate you on how to protect your identity and make you aware of new trends in cyber crime.

Top Holiday Phishing Scams & Practical Safeguards

Here are some of the top Holiday phishing scams that you may encounter and some steps that you can take in protecting your identity and safeguarding your bank account!

- **Fake Purchase Invoices**
 - Clicking on fake receipt links in emails can inadvertently install malware or take you to a phishing site landing page that will ask you to enter personal information!

iTunes Store
To: [REDACTED]
Your invoice: [REDACTED]
12 February 2015 18:00

Beware of scams like this

Order ID: [REDACTED]
Receipt Date: 12/02/2015
Order Total: GBP 22.99
Billed To: Credit Card

All links are to phishing sites

Item	Category	Type	Unit Price
Space Qube Write a Review Report a Problem	Game	iOS APP	GBP 22.99
Order Total:			GBP 22.99

BEWARE

- Shipping Status Malware Messages
 - These are similar to fake purchase invoices in that clicking on any of the links contained in the email can inadvertently install malware or take you to a phishing site landing page that will ask you to enter personal information!



We have sent you a message with the required information.
[Click here](#) to open this email in your browser.

Thanks for choosing FedEx®.

More details

- **Email Deal Advertisements**
 - Not all email sales flyers are going to be legitimate
 - The most obvious fakes are from sites/stores that you have never visited or done business with before
 - Even recognizable name-brand stores can have their email flyers spoofed by hackers and sent out with malware attached or phishing site links contained in the email



- **Inspect Links & URL's More Closely!**
 - It's easy to let your guard down during the frantic holiday season
 - Hover over links in URL's & emails to see where the address is REALLY going to!

- If you are shopping online, make sure that the https “lock” icon is displayed in the URL bar before typing in any personal or credit card information!
- Also look for frequent misspelling of words – a common occurrence in fake emails



- **Keep A Close Eye On Your Accounts!**

- The holiday shopping season is the time of year when it is easiest for hackers & thieves to pilfer your checking, savings, and credit card accounts
- Login at least weekly to all your online-accessible accounts & setup email/text alerts for purchases & balance limits
- Try NOT to use Debit cards that are linked to your savings or checking accounts for shopping – use a credit card instead or you may find entire cash reserves spent



- **Some Other Practical Safeguards**

- Don't use public computers or WiFi to do online shopping

- It may seem trendy & “chic” to shop online at Starbucks, but it’s not worth the risk!
- Don’t respond to popup ads when visiting a website
 - They are often laced with malware & the site owner may not even be aware of them!
- Don’t autosave your credit card info online
 - It may be convenient to do so, but you are playing fast & loose with your credit info!
- If you do create an online account with a merchant, use complex/long passwords
- Don’t walk around the mall (or anywhere for that matter) with Bluetooth enabled!
 - Hackers can “Blue-Jack” the info stored on your smartphone by following you around
- Use an RFID-proof wallet or wrap your credit cards in Reynolds Wrap
 - Hackers can scan your credit card info with an RFID scanner

Hopefully this will give you a few practical tips on having a safe and sane Holiday shopping season. After all, nobody wants to fall prey to the many “scrooges” out there who are lurking in the cyber shadows waiting for an unsuspecting victim. Be aware & be safe!

Paul T. Yoder
Information Systems Security Specialist
El Camino Community College District
pyoder@elcamino.edu