

First Friday Fraud Facts+

June 6, 2014



QUESTIONS OR COMMENTS:

Chris Floyd, CPA
Financial Specialist
P.O. Box 83720
Boise, ID 83720-0011

Phone: (208) 332-8814
Fax: (208) 334-3415
E-mail: cfloyd@sco.idaho.gov

Inside this issue:

Welcome	1
What are E-scams?	1
Phishing	1
Protect Yourself	2
Tips for Avoiding E-scams	2
What to do if You Are a Victim	2
Fraud Case	3

The Idaho State Controller's Office distributes this newsletter as a cost-effective method of increasing awareness about ways to detect and prevent fraud, waste, and abuse in government.

Welcome to First Friday Fraud Facts+ (F4+). This edition will discuss E-scams.

WHAT ARE E-SCAMS?

Fraudsters are more enterprising than ever, using technology to their advantage and our loss. E-scams are fraudulent activities promoted electronically. Many scams are perpetrated through email; others occur at the point of sale, whether online or in person. Criminals look for weaknesses to exploit, whether a trusting individual that clicks on a link, or someone who is careless with the security of their financial information. With summer just around the corner, take a moment to think about how you plan your summer vacation, where you look for bargains, and how you make your purchases.

PHISHING

Many e-scams come through your email. Phishing emails are those that are exploring (fishing) for a quick way to part you and your money or financial information. Examples include:

- Asking you to click a link or open an attachment which may contain a virus
- Offers for quick cash for forwarding packages, accompanied by fraudulent money orders sent
- Links in email supposedly from your financial institution asking you to provide personal data
- Too good to be true deals with offers or email links to fraudulent websites which capture your personal information

Some consequences of following the requests in the phishing emails are:

- Never getting the goods you ordered
- Credit card information stolen and subsequent fraudulent purchases made
- Malware or virus installed on your computer¹



PROTECT YOURSELF

In order to protect yourself and ensure a positive purchase, consider these tips for safe email:

- Don't open unsolicited email or open attachments within
- Don't click on links in unsolicited email
- Be wary of emails that request personal information
- Be cautious of emails that pressure you to act immediately – this usually signifies a scam

TIPS FOR AVOIDING E-SCAMS

Whether you travel for your summer vacation or relax at home, follow these tips for safe shopping:

- Review credit card statements weekly, not monthly
- Monitor bank accounts regularly
- Review credit reports – you are entitled to one free per year from each of the three credit reporting agencies
- Identify accounts on the credit report in your name which you did not create
- Shop online only at reputable retailers
- Scrutinize the retailer's web address to ensure the URL is legitimate; look for misspellings or extra characters
- Ensure the URL is HTTPS, indicating a secure website for accepting payments

Finally, be sure your computer operating system is up-to-date with the latest security patches. Install and maintain anti-virus software and firewalls on your computer, and scan any files before downloading to your computer.

WHAT TO DO IF YOU ARE A VICTIM

- File a complaint with the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center at <http://www.ic3.gov/default.aspx>
- Contact your local FBI office
- If you receive spam or unsolicited email offers, forward to the Federal Trade Commission at spam@uce.gov¹

FRAUD CASE

A woman in the Los Angeles area was arrested in early March 2014 for stealing the personal information of hundreds of people. The woman, Reon Jordan, formerly worked for a medical billing company, giving her access to personal identifying information and credit card numbers. She had more than 200 stolen credit card numbers when arrested.

Jordan used this information to create more than 400 identity profiles. She used the credit cards to pay for tuition at West Los Angeles Community College after she lost her job. In addition to paying for college tuition, Jordan also bought clothes, jewelry, airline tickets, and hair extensions. The charges, in addition to unauthorized use of personal identifying information, include grand theft and burglary. Jordan's bail was set at \$1.2 million.²

¹New E-Scams & Warnings. "Holiday Shopping Tips" Federal Bureau of Investigation (November 26, 2013). <http://www.fbi.gov/scams-safety/e-scams> Accessed Jan 10, 2014.

²Identity Theft 911. "Identity Thief Stole Credit Card Info to Pay for College," (March 5, 2014). <http://www.idt911.com/KnowledgeCenter/NewsAlerts/NewsAlertDetail.aspx?a={86AC39D8-6528-45EB-9848-CB5C3B4D82F1}> Accessed April 9, 2014.

