

First Friday Fraud Facts+

February 6, 2015



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
The Dangers Defined	1
How to Protect Against Security	1
Have a Plan	2
Announcements	2

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 securing laptops and mobile devices.

Laptops and mobile devices are becoming more common for personal and business use. Along with increased use, the risk of theft, malware, and fraudulent lures has increased as well.

The Dangers Defined

The ways some of these threats are carried out are:

- Theft—Taking of an item when it is left unattended, without the owner's permission. The thief is hoping for a device that is unsecured and contains lots of data.
- Malware—Software programs which damage or do unwanted actions to your computer system and/or mobile device. Examples of malware include viruses, worms, trojan horses, and spyware.
- Fraudulent lures—To convince an unsuspecting person to click or navigate to harmful sites. This can be achieved through emails, text messaging or any other means. SMS spoofing is an example of a fraudulent lure deployed by a mobile device.¹

How to Protect Against Security Threats

Listed below are some basic security measures one can take to help prevent these risks.

- Using a password—Passwords on your laptop or mobile device are a first line of defense to alleviate the risk of data theft.
- Use secure email—By using secure email, your username, password, and email contents are encrypted as they travel across the internet.
- Use a virtual private network (VPN)—The VPN encrypts the data between your computer and your office network to protect the data from other network users.
- Keep your device physically secure—Lock your laptop; don't leave your device sitting in the open. This removes the opportunity for



thieves to steal your device and gain access to your information.²

- Use apps—Protect your mobile device with antivirus apps, phone locators, and remote app wipes.
- Be cautious—Be cautious when installing third party apps to your device, some may not be legitimate.
- Use Wi-Fi wisely—Only transmit sensitive data on a secure Wi-Fi. Using public Wi-Fi to transact business could increase the risk of someone stealing your data or viewing sensitive information.
- Keep software programs and apps up-to-date—Neglecting to keep software programs up-to-date may give hackers an opportunity to use past vulnerabilities to get to your information.³

Have a Plan

The use of mobile devices has made it possible for work outside the office. If your office allows the use of mobile devices, it's important to have a security policy. Know what data needs to be secured in order to help prevent data or device loss. Storing sensitive data increases the need to have a plan and know how to keep the data secure.⁴

¹ Malware. <http://techterms.com/definition/malware>. Accessed January 9, 2015.

² Tip: How to secure your laptop data. <http://usatoday30.usatoday.com/tech/news/story/2012-02-19/secure-laptop-data/53136014/1>. Accessed January 10, 2014.

³ Keep your phone safe. How to protect yourself from wireless threats. <http://www.consumerreports.org/cro/magazine/2013/06/keep-your-phone-safe/index.htm>. Accessed January 10, 2014.

⁴ How to secure business mobile devices: a safety checklist. <http://www.techradar.com/news/world-of-tech/management/how-to-secure-business-mobile-devices-a-safety-checklist-1276036>. Accessed January 9, 2015.

ANNOUNCEMENTS

1) Mark your calendars to attend one of the following Annual Internal Control Training sessions presented by the Idaho State Controller's Office:

a) Tuesday, April 14, 2015, from 9:00 a.m. — 11:00 a.m.

OR

b) Wednesday, April 15, 2015, from 9:00 a.m. — 11:00 a.m.