

Security Matters

Focus on Phishing

In this ever-changing information age of social media and digital technology, we as public servants and employees of the State of Montana must be vigilant to guard against the continual barrage of attacks we encounter from cybercriminals. Despite all the resources and vigilant efforts we allocate to secure the State's network and assets, one malicious email or phone call from a cybercriminal can be catastrophic to an employee or our systems.

Cybercriminals may attempt to install malicious software or gain access to your personal information under false pretenses. Two common methods used by cybercriminals

are through Phishing email or phone calls. Phishing is a term used to describe the process of an individual attempting to use social engi-



neering to manipulate confidential information from an employee. Most often, this information revolves around

access to network credentials such as user-ids, passwords, social security numbers, and banking information such as bank account numbers or credit card numbers, usually with the intent of committing some sort of fraud such as identity theft or gaining privileged access to an information system.

One of the best ways to avoid being a victim of a phishing attempt is to validate the information from the sender. Examples:

- ◆ Are you expecting a package to be delivered from UPS or FEDEX?

[Continue on page 5](#)

Security Sessions at the Montana Government IT Conference

The 12th Annual Montana Government IT Conference will be held December 7-11, 2015 in Helena. This year security will be a big part of the conference starting with Trustwave doing a full day of training on Web Application Firewall Architecture and Best Practices on Monday, the 7th. Ten sessions will focus on security on Wednesday and Thursday.

Digital Security

Many components go into creating and maintaining an effective security program, including policies, standards, training, and best practices. Jayne Friedland Holland will talk about NIC's

security culture and highlight the key components of its security program that promotes the protection of its business and government partners.

Tools of the Trade

There are many popular network security tools in use on SummitNet. This session will explain these tools and how they are used on our network.

Starting with Security Introduction to creating a security program with a focus on policies and basic, high impact, and steps to take for securing IT systems.

Effective Security Training and Awareness Programs

You've probably heard it said, "people are the weakest link in security" and there's a lot of truth in that. While security awareness programs are often required to meet compliance regulations, how do you create a program that goes beyond "I'll do it because I have to" to a program that engages users and makes an impact? How do you create a culture where people understand and want to be secure? This session will focus on how to make information security awareness programs interesting, fun and educational.

[Continue on page 2](#)

Security Matters is the monthly information security newsletter published by the Enterprise Security Program. Each month we also have a supplemental file of materials you can use for security awareness. You can find that file at: <http://sitsd.mt.gov/Montana-Information-Security/Security-Training-Resources>

We hope you'll find the newsletter and materials useful and hope you'll give us feedback on what we can do better. Your suggestions for topics and content are welcome. [Contact us.](#)

Inside this issue:

Current Threats & Vulnerabilities	2
MT Information Security Advisory Council	3
Security Event Calendar	3
OPM Issues Notification Letters	4
Holiday Awareness Videos	4
Security Training News	5
Training Resources	5
Security Event Prize Winners	6
News You Can Use	7



A monthly update on the latest security threats and other software news.

- Sean Rivera, CISSP

Security Bug in Dell PCs

Information Security experts have identified a security flaw in new Dell laptops and desktops that have shipped since August 2015. These systems have a self-signed root certificate that includes the private cryptographic key for the certificate which, if exploited, could lead to malicious users to intercept, read, and modify web traffic for the unsuspecting user.

The certificate in question, eDellRoot, can be removed from the operating system's trusted root certificate authority. Agencies that deploy their devices with images built from the ground-up shouldn't need to worry about this certificate being present. But those of us who perform IT troubleshooting on behalf of our families, friends, and colleagues may wish to take a closer look at this issue.

For more information, please

see:

<http://krebsonsecurity.com/2015/11/security-bug-in-dell-pcs-shipped-since-815/#more-33044>

<http://arstechnica.com/security/2015/11/dell-does-superfish-ships-pcs-with-self-signed-root-certificates/>

Popular Facebook App a 'Privacy Nightmare'

If you are one of approximately 17 million users of the popular "Most Used Words" Facebook application, you might consider uninstalling the application as soon as possible. Here's a list of everything the app requests access to:

- Name, profile picture, age, sex, birthday, and other public info
- Entire friend list
- Everything you've ever posted on your timeline
- All of your photos and photos in which you're tagged

- Education history
- Hometown and current city
- Everything you've ever liked
- IP address

Info about the device you're using including browser and language

The app's policy states that information could be stored on servers on "any location" in the world, meaning that your data may reside in countries with poor or non-existent privacy laws. Additionally, and unfortunately, the privacy policy for this application states that they "may continue to use any non-personally-identifying information" after a user deletes the app. The creator of the application has not made any public comments about these findings yet.

It is a good practice to always review permissions and privacy settings before installing applications and to deny any that seem unnecessary or excessive.

[Conference continued from page 1](#) **Digital Forensics**

A panel discussion about how the Digital Forensics services from both SITSD and DOJ can assist customers with both criminal and non-criminal investigations relating to both user activity and security incidents for the State of Montana. The panel will distinguish the boundaries in which SITSD and DOJ can perform Digital Forensics. SITSD's portion will share some information of the trends in malware seen on devices and provide some ideas on how to mitigate infections. Plenty of time will be saved to allow questions.

What is Splunk and What can it do for me

Splunk can monitor and analyze anything and everything, from customer clickstreams and transactions to security events and network activity. Splunk aggregates system, network, and securi-

ty data to enable analysis from end-to-end. From troubleshooting to optimizing, Splunk gives you a single interface for searching logs and correlating events so you can better understand, manage, and secure your environment. The first half will cover architecture, data onboarding, and data searching followed by a Q&A session.

Source Control Best Practices

Source Control overview and why SITSD offers this essential service with a focus on Subversion, SITSD'S hosted solution. Discussion on similarities and differences between Subversion and other source control products on the market such as Git and Team Foundation Server. Introductory topics will include backup and recovery, versioning, repository snapshots, team collaboration, conflict resolution, security and accountability. Also covered will be how SITSD's internal develop-

ment team uses source control to manager agile iterations smoothly, efficiently and effectively. This will transition into advanced topics that include branching/merging and tagging.

Introduction to System Security Plans and Risk Assessments

This panel will focus on concepts related to implementing a risk management strategy that complies with State of Montana statutory law, State of Montana enterprise security policies, federal regulations, and industry best practices. Additionally, this panel will provide helpful example templates and working strategies from agency officers that have been using these concepts in actual practice.

Physical Points of Intrusion

Physical door security. How easy is it to enter your "secure" areas physically? See how simple it may

be, and cheap ways to secure.

Varonis – Protecting your information from the Inside Out

Target lost 40,000,000 records in a 2014 breach that cost them \$148 million dollars. Ouch. They had lots of fancy tools watching the perimeter, but fell short when it came to securing insider access. Protecting against insider threats, whether malicious or accidental, is extremely difficult, especially when 71% of employees say that they have access to information that they aren't supposed to see. Join us for a live presentation where you will learn six tactics for preventing insider threats.

The conference wraps up Friday with a **Cyber Table Top Exercise** hosted by the Department of Homeland Security.

[More information and registration.](#)

Meeting Highlights of the Montana Information Security Advisory Council Meeting & Preview of the Upcoming Meeting



November 18, 2015 Meeting highlights

The MT-ISAC discussed the MT-ISAC Workgroup Model which will be published in early December. The discussion centered on workflow within the workgroups.

It was decided that the Enterprise Security Program (ESP) is already providing outreach and training and awareness services so no workgroups to address those areas will be formed at this time. The ESP will provide quarterly updates to the Council.

Workgroup Updates

Assessment:

The Assessment workgroup is working on an assessment document for tracking compliance to Information Security Policy. The draft document will be presented during the January MT-ISAC

meeting for member review.

The workgroup also discussed ideas for Governor's Dashboard. There were a variety of different scenarios for a dashboard. The workgroup will work with Governor's office on those different scenarios and what they would like to see.

Other discussion focused on the plan for using MS-ISAC's National Cyber Security Review tool based on the NIST Cyber Security Framework as a yearly assessment for each agency to be included in MT-ISAC yearly reporting to the Governor.

Best Practices:

Several members traveled to Seattle to tour the State of Washington National Guard Cyber Unit and will give a report at the January meeting.

The workgroup is gathering infor-

mation on the following:

- Device hardening;
- Disposal of devices;
- Encryption of data at rest;
- Sharing of documents outside the State and within;
- Password storage; and
- Security devices while traveling outside the country.

Situational Awareness:

Members spoke to Chief Information Security Officer (CISO) from State of Pennsylvania at MS-ISAC Annual Meeting in San Diego about the State of Pennsylvania's Fusion Center and its situational awareness program. They may have a meeting in January to further this discussion on learning more of the State of Pennsylvania's best practices in situational awareness and how it would fit within our environment.

The workgroup had a discussion on incident response and re-

porting and how to improve agencies' communications in this area. Several incident response forms were discussed.

It was decided to use the Network Managers Group (NMG) meeting held every Friday at 9AM to discuss situational awareness and share information. This will be the first agenda item each meeting.

Other Business

Joe Frohlich provided an overview of the Montana Government IT Conference security sessions. The list of sessions has been posted to the [MT-ISAC website](http://mt-isac.org). Register for the conference at <http://itconference.mt.gov/>

There will be no December meeting of the MT-ISAC. The next meeting will be January 20, 2016 at 1:00 p.m. in the State Capitol, Room 152.

Security Awareness 2015 Events

Focus on Phishing

- ◆ Dec 1, 2015 - 9:30—12:00 at COR EOC Conference Room
5 S Last Chance Gulch
- ◆ Dec 15, 2015 - 9:30—12:00 at DPHHS Sanders Room 107
111 N Sanders St.

Focus on Physical Security

- ◆ Jan 27, 2016 - 10:30—1:00 at FWP Conference Room
1420 E 6th Ave.

Check [Montana Information Security](http://mt-isac.org) for the latest event schedule and don't forget to come see us at the [Montana IT Conference](http://mt-itconf.org) December 7-10, 2015.

U.S. Office of Personnel Management Issues Notification of Cyber Incident and Protection Services

Some State of Montana employees and former employees have begun receiving notifications from the U.S. Office of Personnel Management (OPM) stating that their data was compromised in a cybersecurity incident discovered in June 2015. These letters have been going out at a rate of about 800,000 per week and OPM expects to complete the mailing in mid-December, so if you have not received a letter it is possible you still may.

The letter details what data may have been compromised and the protections that are provided for those affected, including credit and identity monitoring, identity theft insurance, and identity restorations services. The letter includes a PIN which is needed for enrolling in the services, so it is important not to throw this letter away.

The Information Systems Security Office (ISSO) has received some questions about the legitimacy of these letters and provides the following tips for validating the letter:

- The letter arrives as a sealed privacy mailing, similar to mailings containing the PIN number for a credit or debit card.

- It bears the seal of the U.S. Office of Personnel Management.
- It addresses the recipient by name.
- It contains a five part PIN.
- It contains a website address for enrolling in the services and phone number for calling with questions.

We have heard of scams connected with the OPM incident, including phone and email contact offering free credit services. Please note that OPM and companies acting on their behalf will NOT use email or phone to contact you to offer services. Neither will they contact you to confirm personal information. If you are contacted via email or phone or asked for personal information do NOT provide it.

For more information, including sample notification letters please visit <https://www.opm.gov/cybersecurity/#Services>



Security awareness doesn't have to be boring. The Security Awareness Company does some great videos to get the word out. Two of them are especially fun during the holidays. Enjoy and share with your family and friends! (Click on the picture to go to the video.)



Online We Will Go - Jingle Bells Cyber Safety Parody



1,419



Dreaming of a Clean Email - Dreaming of a White Christmas Cyber Safety Parody



634 views

[Focus continued from page 1](#)

- ◆ Have you heard about an increase in mailbox sizing from your email administrators?
- ◆ Do you know the person or recognize the originating email address?
- ◆ Pay attention to spelling and grammar. Cybercriminals sometimes have poor spelling or grammar.
- ◆ Beware of links in email. If you see a link in a suspicious email message, don't click on it.
- ◆ Cybercriminals often use threats that your security has been compromised.
- ◆ Spoofing popular websites or companies. Scam artists use graphics in email that appear to be connected to legitimate websites but actually take you to phony scam sites.
- ◆ If it sounds too good to be true, it probably is.



Remember, no parcel delivery

service will send you an email regarding an undeliverable package, and in order to increase your inbox size, your IT staff does not need your user id and password to do so. That leads us to evaluating a suspicious email.

First, always review the sender's email address. Do you really believe that someone from some random university or business is going to contact you about upgrading your inbox?

Not all emails are equal, though, and there are some that are incredibly convincing.

If you receive an email regarding an offer from a vendor or retailer, best security practices suggest not clicking the link within the email. Instead, open your web browser and manually navigate to the vendor or retailer's site to validate the offer. Other means of verifying addresses on a link include hovering your mouse over the link to see where it points, as well as copying the link and using a site such as URLVoid.com to check a website's reputation.

Telephone phishing attacks are on the rise as well. Often, these calls come in the form of an individual pretending to be from a tech company, most often Microsoft, and reporting to you that they have detected malware running on your computer. They then offer to help and attempt to manipulate the



user to create a remote connection with them to remediate the problem. Doing so allows the attacker to gain access to the system, install malware and key loggers, and potentially steal other important data. Microsoft will never legitimately contact a user to address malware infections, nor any other 3rd-party technology company.

Another telephone phishing scam claims to be from your bank, credit card company, or other financial institutions. They tell you that your account has been compromised and ask for account information so they can resolve the issue for you. Remember that financial institutions will never ask for your account and personal information over the phone.

Other telephone phishing scams center around the use of "bullying" the victim into providing a payment to avoid litigation.

These accusatory types of calls center around back-taxes, unpaid speeding tickets, or other legal fines, and attempt to extort credit card numbers or bank account information from their targets.

On any of these types of calls, it is advisable to just hang-up.

Regardless of how convincing the person on the other end of the phone is, never provide any personally identifiable, account, or address information. If you have any questions or think the call may be legitimate, look up the contact information for whoever called you in your records and contact them directly. Do not call back a number provided by the original caller.

If you are unsure about the validity of any emails or phone calls, you should request help from your IT Security staff to help determine the legitimacy of the information.

Congratulations to the prize winners at the October and November Security Awareness Events.

Gift cards:

- Ed Sivils
- Priscilla Sinclair
- Suzi Kruger
- Mark Van Alstyne
- Dan Olson
- Ian Lyon
- Ed Soto



- Kristie Rhodes
- Patrick Boyle

- Barry Wall
- Tim Kosena

- Patty Hoover
- Shane Gilbert
- Matt Goldsworthy
- Gary Martinsen
- Mary Buswell
- Kathleen Johnson

The monthly grand prize winners of an auto emergency kit are:

- Dave Powell
- Jordan Lillibridge

News You Can Use—Just In Time for the Holidays

17 Ways to Prevent Identity Theft When Traveling

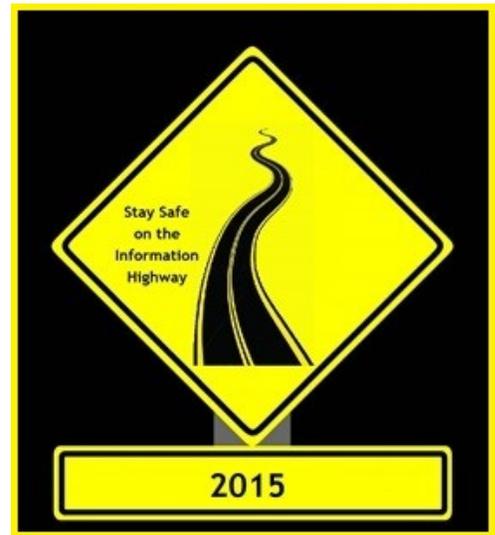
Some great advice from Robert Siciliano on steps to take to prevent identity theft while traveling.

Tips for Safe Online Shopping In The Age Of Hackers

Although Black Friday and Cyber Monday are behind us now, there's still plenty of shopping to be done for the holidays. Here's some advice to help you keep your data safe.

Amazon Enables Two-Factor Authentication (And So Should You!)

Amazon is offering a new security option to help protect the security of your Amazon account.



Security Quick Tip

Don't get hooked by phishing:

- * Hover over hyperlinks to see where they will take you.
- * Be wary of urgent requests asking you to provide information or update accounts.
- * If it sounds too good to be true, it probably is!

For more security tips, news, advisories, and resources visit the Montana Information Security website, find us on Facebook, or follow us on Twitter.

<http://sitsd.mt.gov/MontanaInformationSecurity>

 State of Montana Information Security

 @MontanaSecurity

Contact Us:

[Enterprise Security Program](#)

[Lynne Pizzini, CISO and Deputy Chief Information Officer](#)

[Joe Frohlich, Enterprise Security Manager](#)