

Security Matters

Focus on Physical Security

We spend a lot of time at our desks each day. Whether our desks are neat as a pin or a chaotic mess, we should all have an awareness of what office habits are security risks and how to protect ourselves, our customers, and our employer from theft of information, identity, or property. As you look around your workspace, here are some suggestions for making it more secure.

Unlocked computers

Unlocked computers can enable unauthorized access to the information systems for which you have access as well as to sensitive documents on the device or network connected drives. If you going to be more than a few steps away from your desk, lock your computer.

Unsecured tablets

It's easy for a thief to walk off with a tablet or laptop – and in



turn, all the data stored on the device. Tablets and laptops should be either stored in a locked drawer or cabinet or taken with you when you leave for the day, as well as during extended absences from your desk during the day.

File drawers and cabinets

Confidential or sensitive files should not be left out on the desk when you are away. Put them away except when you are working at your desk. Folders can easily be taken from an unlocked file cabinet. And if the keys are available to be copied, files can be taken, copied, and returned with you none the wiser about the theft. If you have any sensitive information in your file drawer, keep it locked and keep the keys with you.

Binders containing confidential information should not be stored on open book shelves. Keep them in locked cabinets or rooms with restricted access. Consider installing a second locking mechanism on any file cabinets that contain confidential information.

Data Privacy Day

Data Privacy Day (DPD) is January 28th of each year. In the United States it began in 2008 as an extension of the same celebration in Europe. DPD commemorates the 1981 signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection. In 2014, Congress adopted Senate Resolution 337 expressing support for January 28 as “National Data Privacy Day”.

DPD’s aim is to create awareness about the importance of privacy and protecting personal information. Under the leadership of

the National Cyber Security Alliance (NCSA), public and private businesses, schools, and governments come together to promote data privacy in traditional media, social media, and events through-



out the country, as well as support privacy research.

You can get involved to help create a culture of privacy awareness. Start by becoming a DPD Champion and receive a free toolkit to help you spread the word. Sign up at <https://www.staysafeonline.org/data-privacy-day/champions/>. Both individuals and organizations can sign up.

For more information on how to get involved and promote DPD visit <https://www.staysafeonline.org/data-privacy-day/landing/>.

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
Security Event Calendar	2
MT Information Security Advisory Council	3
Security Training News	4
Training Resources	4
Free Professional Training Opportunity	5
Cybersecurity New Year’s Resolutions	5
Awareness Event Prize Winners	6
News You Can Use	7



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

- Sean Rivera, CISSP

DON'T BE A VICTIM OF TAX FRAUD IN 2016

As has become a recurring theme for the past several years, both the IRS and state-governments are getting ready to fight off the hoard of identity thieves that make a living on fraudulent tax refunds. Tax refund fraud affects hundreds of thousands of US citizens annually. Victims typically learn of the crime after having their returns rejected because a scammer has beaten them to the punch on submitting their returns. Thankfully, the IRS has improved its ability to detect and deny fraudulent returns. In 2013, the IRS blocked fake refunds in the amount of \$24.2 billion dollars. Note that was “B” as in BILLION. On the flip side, though, is that the IRS paid out an estimated \$5.8 billion fraudulently that year.

Sadly, in this day and age, identity theft is rampant due

to the ever-increasing number of data breaches. So how does one avoid becoming a statistic to tax-fraud?

File before the fraudsters do –
The best defense is to file your state and federal taxes as quickly as possible. The tax season starts January 18 this year, so be ready. Remember that it doesn't matter if the IRS owes you money. A fraudster can submit a claim that says you do, and leave you with the burden to sort things out with the IRS.

Get in the habit of requesting your free credit report – By law, consumers are entitled to an annual review of their credit reports for free from each of the major credit-reporting bureaus. Request a copy from a credit bureau once every three to four months. Remember that there are 4 major companies, so keeping track of one every quarter should

be sufficient to reveal any red flags.

Monitor or possibly freeze your credit file– Take advantage of any free credit monitoring available to you and then freeze your credit file to prevent misuse. Here is a recommended article to read regarding this practice: <http://krebsonsecurity.com/2015/06/how-i-learned-to-stop-worrying-and-embrace-the-security-freeze/>

File a Form 14039 and request an Identity Protection (IP) PIN – This form requires consumers to state they believe they have been or are likely to be victims of ID fraud. Even if one has not experienced a fraudulent tax returned filed on their behalf, virtually all Americans have been touched by compromises and breaches that could lead to ID theft.

Security Awareness 2016 Events

Focus on Physical Security

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

Focus on Identity Theft

- ◆ Feb 9, 2016 - 10:30—1:30 at DOC Conference Room 228
301 S Park Ave.



We do not have a March event scheduled yet. Please contact [Lisa Vasa](#) if you'd like to host an event in March—or any other month—at your location. The focus topic is cyber espionage. We do all the work as well as provide treats, giveaways, and prizes. All you need to do is schedule a room and do a little bit of promotion (and we help with that, too). We make it easy and fun for you to bring security awareness training to your agency!

Check [Montana Information Security](#) for the latest event schedule

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



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

The MT-ISAC workgroups did meet during the month of December and here is a summary of those meetings.

Assessment Workgroup

This workgroup is tasked to develop a standardized plan of action to accomplish agency compliance to the Information Security Policy and the reporting of progress to the State CIO. Other tasks are to develop a Governors information security dashboard as well as a yearly security report to the Governor's Office. Lynne Pizzini is Chair of this workgroup. This workgroup meets the first Wednesday of each month.

- The Assessment workgroup met on December 2nd and reviewed an early draft of the assessment document where there were positive comments from the workgroup on the document. The workgroup will continue to develop the document and present a more finalized ver-

sion during the next workgroup meeting. This finalized workgroup assessment document will be then presented to MT-ISAC in January.

- The Assessment workgroup is going to recommend using MS-ISAC/Center for Internet Security's National Cyber Security Report (NCSR) to be used as the yearly report to the Governor's Office. The NCSR is reflective of the Enterprise Information Security Policy and is a quick way to gauge where an agency currently stands to national standards within security.
- The Assessment workgroup also discussed several ideas for the Governors Dashboard. Lynne Pizzini will work with the Governor's Office to discuss these ideas.

Best Practices Workgroup

This workgroup is tasked to seek national standard best practices within security and apply them in Montana where applicable. Lynne Pizzini is Chair of this workgroup. This workgroup meets the first Thursday of each month.

- The Best Practices workgroup met on December 3rd. Current topics being discussed are Device hardening, disposal of devices, encryption of data at rest, incident response, sharing of sensitive documents outside of state network and within, password storage, securing devices while traveling outside the country.
- Device hardening and disposal of device's documents should be finalized by the next workgroup meeting and then presented to the MT-ISAC in January.
- There was a discussion on using AirWatch and using factory reset on BYOD devices. Using AirWatch is the enterprise solution for BYOD, doing a factory reset of the device is only solution known at this time for state owned cellphones and tablets. It was suggested to destroy these state owned devices at end of life.

Situational Awareness Workgroup

This workgroup is tasked with increasing the awareness of current threats and to foster communication to best deal with these threats. Bryan Costigan is Chair of this workgroup. This workgroup meets the fourth Wednesday of each month.

- The Situational Awareness Workgroup met on December 16th. Incident Response forms were discussed where there might be a need for two possible standardized forms, one for low level IR events and one for more critical event. Social engineering was also discussed and it was identified that more training and enterprise standards are needed in the area of Incident Response and social engineering. Possible idea of have tabletop exercises to train in these areas.

The MT-ISAC encourages participation from all interested persons. One way to get involved is to join the workgroups. If you are interested in joining any of the workgroups please contact Joe Frohlich at jfrohlich@mt.gov.



NEW MT-ISAC SharePoint Site

The Montana Information Security Advisory Council now has a [MT-ISAC SharePoint site](#). This SharePoint site is only available to those who have state active directory credentials at this time. The [MT-ISAC website](#) will still be where agendas to meetings and approved documents will be stored. For more information contact the [Enterprise Security Program](#).

Security Training News



SANS Annual Winter Buy

The Center for Internet Security and ANS are once again offering SANS's information security training at up to a 70% discount during the Annual Winter Buy Period, December 1, 2015 to January 31, 2016.

Among the available training are the SANS OnDemand and vLive technical training courses. Vouchers for the courses are \$2475 each and there is a minimum purchase of three. (The minimum ap-

plies to all State of Montana purchases. It is not by individual agency.)

SANS Securing the Human for Developers is also included in the discount. This training is designed to provide software security awareness for everyone involved in the software development process. Licenses are \$250 each, with a minimum of 10 licenses.

The Enterprise Security Program has purchased some licenses for the STH Phishing tool which they will be using

to conduct phishing tests. If agencies wish to purchase additional licenses for use within their own agency, the price during the buy period is \$1.90 each for one year or \$3.30 for two years.

If you are interested in purchasing training, or phishing tool licenses, please contact Lisa Vasa (lvasa@mt.gov) by



January 15, 2016.

FREE Security Professional Training

We're always on the lookout for free training and this month we happened on Cybrary: "We believe IT and Cyber Security training should be free, for everyone, forever. We believe that everyone, everywhere, deserves the OPPORTUNITY to learn, primarily because everyone is essentially forced to use internet enabled devices." While we haven't had a lot of time to test drive the courses yet, there is a lot of material here for both new and experienced security staff. Check them out at <https://www.cybrary.it/>.

FedVTE Live! Cybersecurity Investigations

Virtual Class—January 26 or January 28 7:00 AM to 3 PM

The Department of Homeland Security (DHS) is hosting a single-day, hands-on course that teaches students the basic concepts of cybersecurity and digital forensics investigation practices. Students will learn how to perform collection and triage of digital evidence in response to an incident. Students will perform hands on activities throughout the day to reinforce discussions on building response capabilities, forensics concepts, evidence collection methodology, volatile data collection, and forensic best practices. Students will perform limited analysis to identify additional avenues of investigations and collection. **Applications and pre-tests must be submitted to DHS by January 13, 2016.** If interested, please contact Lisa Vasa for course information and the application form.

What's New for Security in Windows 10 and Server 2016?

Virtual Event — January 11 8:00 AM MST

What's new in Microsoft's latest operating systems? Window 10 has 3D facial scanning for biometric logins, new ways to protect credentials in memory, plus a new browser to replace Internet Explorer. Server 2016 has Docker containers, Server Nano, virtual TPMs, PowerShell 5.0, and more. Attend this free webcast from "The Windows Guy" at SANS, Jason Fossen. Jason is not a Microsoft employee, so get the straight story here. [Registration](#)

2016: Examining the Threatscape Ahead

Virtual Event—January 20 9:00 AM MST

How is the landscape changing for cybersecurity and what do businesses need to know to protect themselves? From large scale data hacks to credit card breaches, Sr. Security Researcher, Stephen Cobb, looks at the major trends in cybersecurity for the upcoming year and discusses the tools and resources available to protect against them. [Registration](#)

For more security training and awareness resources, check out the [Security Training Resources](#) page and watch for more information here each month.

Free Professional Security Training & Certification Opportunity

(Time Sensitive)

The State of Montana has recently created an Enterprise Security Program. This program develops strategies and establishes the overarching framework for securing information systems in state government. One of the programs strategies is to strengthen the State of Montana's Enterprise training and awareness program. Currently all state executive branch employees as well as most other state employees take the SANs Securing the Human training annually. This has been very helpful in developing a more security conscious end user.

There is also an ever growing need to develop the security professional workforce here in Montana. The Enterprise Security Program has recently won a small grant from Department of Homeland Security to fund online security professional training through MS-ISAC's Trusted Purchasing Alliance. Due to the size of the State of Montana and without a large metropolitan city, online training is a great way to extend professional security training throughout the state.

The Enterprise Security Program will coordinate with State, Local and Tribal agencies to select up to six individuals in key strategic security areas for professional security training.

The Enterprise Security Program will pay for the training and exam for certification through this grant. The Enterprise Security Program will select at least one Local Government user as well as one Tribal Government user. The security professional training will be online from your choice of either (ISC)² or SANS. The total cost for this professional online training plus the exam can be up to \$3,200. For more information on (ISC)² or SANS online professional security training;

[\(ISC\)² Online Courses](#)

[MS-ISAC Trusted Purchasing Alliance information on \(ISC\)² training](#)

For additional questions on (ISC)² courses please call Kyle Oliver at (ISC)2 at (703)637-4413.

[SANs Online Courses](#)

For additional questions about the SANs vLive and OnDemand courses, please see the [MS-ISAC Trusted Purchasing Alliance information on SANs training](#).

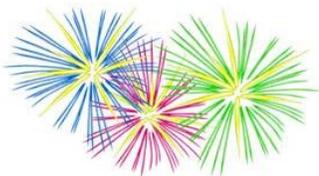
Rules for applying:

- ◆ You must be a State of Montana employee OR State of Montana Local Government employee OR State of Montana Tribal Government employee.

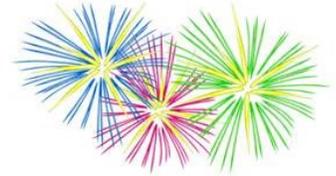
What the Enterprise Security Program is looking for in applications:

- ◆ Motivated person who will dedicate their time to take the online class and to improve their security skills.
- ◆ A short paragraph explaining how this training will help their environment within State/Local/Tribal government.
- ◆ From the links above, choose and state which online course you wish to take.
- ◆ It is encouraged to take the examination for certification, but this is not a requirement. Please state that you either want to take the certification exam or not.

To apply for this online professional security training please email jfrohlich@mt.gov by 5PM January 22nd 2016.



2016 Cybersecurity New Year's Resolutions



Every year people around the world make resolutions about improving their habits, their looks, and their lives so we didn't want to overload you with a long list of cybersecurity resolutions, too. But we couldn't resist suggesting you add these three to your plans for 2016.

Practice good password management.

- * Change your passwords regularly.
- * Use unique passwords for each of your accounts.
- * Create passwords that are more than 12 characters and have upper and lower

case letters, numbers, and special characters.

Protect your devices and data.

- * Keep devices updated and applications patched.
- * Install and use antivirus or anti-malware software on computers, tablets, and phones.
- * Backup your files regularly.
- * Install only the apps you need and make sure to get them from trusted sources.
- * Use a passcode, password, or fingerprint to unlock your device.

Be cyberaware.

- * Don't get hooked by phishing.
- * Don't fall for social engineering.
- * If it looks too good to be true, it probably is!
- * Come to a [Security Awareness Event](#) to learn more.
- * Follow us on [Facebook](#) and [Twitter](#)

Happy New Year from the DOA SITSD Enterprise Security Program and the Information Systems Security Office!

[Focus continued from page 1](#)

ID Badges

Your ID badge provides access into buildings and areas which may be restricted. Prevent unauthorized access by always keeping your badge with you while at work. Better yet—wear your badge!

Passwords

Never write down passwords and if you do, never leave them where others can find them. Do we even need to say why this is a bad idea? If you have too many passwords to easily remember, consider using a password safe or manager.

Keys

Whether the keys are to your car, office, file cabinet, or home, keys should be protected against theft or copying. Always put them away or keep them with you. Never leave them sitting out anywhere.

RSA fobs

For those who are using two-factor authentication, your RSA fob is one half of your authorization to the network. Protect it just like you protect your keys, ID badge, and passwords.

Cell phones

Cell phones have become treasure chest of information, besides be-

ing a target for device theft. Protect your cell phone with a passcode and never leaving it lying around for someone to take.

Portable media

Don't leave portable media like flash drives or external hard drives plugged into your device. Unplug and secure them when you're away from your desk.

Printers and fax machines



Remove documents promptly from the printer or fax. For sensitive data, consider printing a banner sheet to cover the contents.

White boards, bulletin boards, and cubicle walls

It might not be easy to walk away with a whiteboard that's been attached to the wall, but with a cell phone camera a person can quickly walk away with anything written on a whiteboard. Don't leave sensitive information on a

whiteboard, especially if it is visible from hallways or windows.

Briefcases and computer bags

If you carry documents in a briefcase or computer bag, make sure to either lock it or secure it in a locked location when it's not in your physical possession.

Windows

Window exposure can allow re-

sensitive documents. Shred your documents or place them in a locked container until they can be shredded when you dispose of them.

Make sure disposal bins for documents that are to be shredded are securely locked. Check the lid to be sure it isn't so flexible as to allow a thief to reach into the container and pull out documents.

Personal papers and checkbook

Bank statements, personal papers, and checkbooks include personal information and account numbers, leaving you open for fraud and identity theft.

Credit card

How easy would it be to take this credit card and put it to use? Most of us don't use a business credit card on a daily basis so we might not realize it's missing for a while. Keep your credit card in your wallet or in a locked drawer.

Physical security is as important as digital security. Take a few minutes to look around your workspace and make sure you can pass the clean desk test!

Remove documents promptly from the printer or fax. For sensitive data, consider printing a banner sheet to cover the contents. If the monitor is reflected in the window it can allow unauthorized persons inside the office to see the information as well. If your monitor can be viewed through a window, close the blinds when working on sensitive information.

Document disposal

Determined thieves will go through dumpsters looking for



Congratulations to the prize winners at the December Security Awareness Events at the Department of Corrections and the Department of Health and Human Services!

All monthly participants are eligible for the drawings in March and September for Microsoft Surface tablets.

Gift cards:

Chris Matson
Rachel Heaton
Sherri Monson
Dee Glowacki
Val Hartman

Auto emergency kit:

Peter Johnson

News You Can Use

[Social Engineering: How an Email Becomes a Cyber Threat](#)

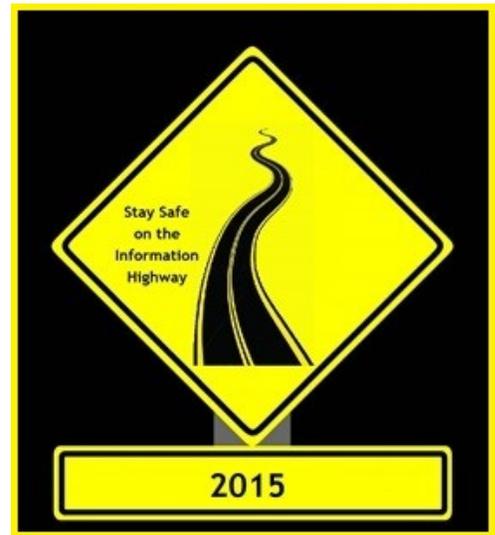
Social engineering techniques are becoming more personalized, advanced, and difficult to detect.

[Cyber Security Predictions for 2016](#)

Steve Weisman, the author of the website [Scamicide](#), makes his 2016 predictions.

[A Hidden Insider Threat: Visual Hackers](#)

We usually think of hackers as distant people working away on a computer. Privacy expert Mari Frank discusses the threat created by a lack of physical security and privacy.



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](#)