

Security Matters

Focus on System Compromise

We talk a lot about what to do to protect our accounts and systems from cybercriminals and malicious activity. It's important to take steps like using strong passwords and multifactor authentication, using caution when visiting websites and reading email, maintaining our applications and devices with patches and updates, and using anti-malware software. Unfortunately, those who would seek to cause harm are constantly hitting us with new attacks every day. The chances that anyone will get their devices or accounts compromised at some point are fairly high. With that bad news ringing in our heads, how do we know when that has happened and what do we do if it has?

Computers and Other Devices

It's likely the first thing that comes to mind when we think about a system compromise is our computer getting hacked or infected. Malware comes in various types with a variety of purposes. Some attempt to use your device as a bot to attack other

devices. Some install spyware which capture information such as passwords and user IDs which can be used by the attacker for more malicious activity. Viruses,



worms, and trojans may destroy files, steal information, or install other programs. Increasingly, devices are being infected with ransomware which encrypts files. To regain access to those files, the user is told he must pay a ransom.

In some cases, like that of ransomware, you'll see a pop-up or a message saying that your device has been compromised. In most other circumstances, the infection won't be immediately appar-

ent. The success of bots and spyware depend on you not noticing the infection. Here are some signs that a device may be infected:

- Slow computer or browser speeds
- Increased CPU usage
- Problems connecting to networks
- Freezing or crashing
- Modified or deleted files
- Unusual files, programs, or icons that you did not add
- Programs no longer running, especially firewalls or anti-malware software
- Emails or messages being sent without your knowledge.
- Strange or unexpected computer behavior.

If you suspect that your work device is infected with any type of malware, notify your Help Desk or IT security staff immediately. Not only are they trained to deal with malware, your device issue may provide information about possible widespread attacks and help prevent [Continued on page 4](#)

Small & Large Incident Handling Documents

The Montana Information Security Advisory Council (MT-ISAC) recently approved the Small Incident Handling document for use by agencies dealing with incidents involving malware infections and other threats to individual devices. While the Enterprise Security Program recommends re-imaging as the most effective way to ad-

dress malware, this document may provide additional insight into investigating and addressing incidents. The document also provides an explanation of critical and non-critical incidents.

The MT-ISAC Best Practices workgroup has also developed a Large Incident Handling docu-

ment. This document has been posted to the [MT-ISAC website](#) for review and will be discussed at the June 2016 meeting. Security and IT professionals interested in incident handling are encouraged to read the document and provide comments to [Joe Frohlich](#) prior to the meeting.

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
	2
MT Information Security Advisory Council	2
Security Training News	3
Training Resources	3
	3
News You Can Use	5



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

Microsoft Wi-Fi sense was introduced into the Windows 8.1 operating system to allow connecting via Wi-Fi hotspots it knows about or shared by your contacts. This was enabled by default at introduction, which caused concerns about privacy and security. Due to low adoption rates, Microsoft will be dropping the application and it will not be present in the Windows 10 Anniversary Update which comes out this summer.

Apple has rolled out patches to resolve the DROWN vulnerability reported in March. The vulnerability stems from a flaw in SSLv2 that could have allowed an attacker to leak user information. Along with the patches to OS X, Apple also issued updates to iTunes and the Safari browser. While it is recommended to keep all systems

and applications patched and updated, it is advisable to back up your files prior to applying updates.

Google has announced plans to phase out all Adobe Flash videos in its Chrome browser by the end of 2016. After the change is implemented Flash content in most web sites loaded by Chrome will be automatically blocked. HTML5 will be the primary content delivery system used in Chrome.

A database dump of 117 million LinkedIn accounts with passwords, user IDs, and email addresses is currently for sale on the darknet. The database is from 2012 and may be outdated. LinkedIn

users are encouraged to change their passwords if they have not already and if not already using it, enable LinkedIn's two-factor authentication. If you have used the same email address and password for other accounts, you should change those passwords as well. This is a good reminder to use unique passwords for each of your accounts.



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



Meeting highlights from May 19th, 2016

National Initiative for Cybersecurity Education

Lisa Vasa discussed a funding opportunity via the National Initiative for Cybersecurity Education (NICE). They are currently soliciting applications from eligible applicants to establish Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS). These RAMPS will identify cybersecurity workforce development pathways for local workforce needs, and will work to promote these educational opportunities by aligning the specific workforce needs of local businesses and non-profits with

the learning objectives of cybersecurity education and training providers. This funding opportunity will provide 5 to 8 grants in the total amount of \$150,000 to \$200,000 each for a fifteen-month project. The applicant must have a letter of commitment from one of each of the following three types of organization: a K-12 school, a higher education institution (if the applicant is not one itself), and a local employer.

Policy Assessment Tool pilot

The agencies participating are: the Department of Administration, Department of Revenue, Department of Transportation, Department of Natural Resources and

Conservation, and Department of Public Health and Human Services. All agencies are welcome to join the pilot. Joe is proposing that the July MT-ISAC meeting be the end of the pilot, at which time the participating agencies will report. Once the Assessment Tool is approved, July 1, 2017 would be the deadline for reporting to the CIO.

Small Incident Handling Best Practice

Council approved the Small Incident Handling document as a best practice. This document is to provide technical best practices on dealing with malware related activity. The Small Incident Handling procedure is posted on the MT-

ISAC website: <http://sitsd.mt.gov/Governance/ISAC>

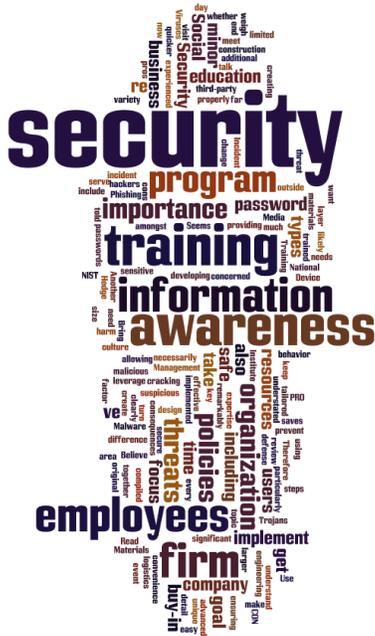
Best Practices up for review by Council

There are two documents for review to be voted on during the June MT-ISAC meeting: The Disposal of Media Storage Device procedure, and the Large Cyber Incident Handling document. These documents are also on the MT-ISAC website.

Next Meeting

The next meeting of the MT-ISAC will be held Thursday, June 16, 2016 from 11:00 a.m. to 1:00 p.m. In room 152 of the Lee Metcalf Building (DEQ).

Security Training News



SANS Summer Buy Window!

The SANS Summer Buy Window is open! From June 1 through July 31 state, local, and tribal governments, non-profit organizations, and public education and healthcare institutions can purchase SANS training courses and programs at discounts up to 70% off the advertised price. This incredible opportunity allows you and your employees to increase your cybersecurity knowledge at a great price.

SANS online professional programs On-Demand and vLive are available during this period. Each course is \$2,475. GIAC certification exams may also be bundled with the course for an additional \$659 each. The minimum purchase is three courses. For more information, please visit: <http://www.sans.org/online-security-training/>

State, local, and tribal governments, non-profit organizations, and public education and healthcare institutions may contact SANS directly to purchase courses, however, due to the minimum purchase requirement, those organizations wishing to purchase less than three courses can contact [Lisa Vasa](#) with the Enterprise Security Program (ESP). The ESP will combine requests from multiple organizations in order to meet the minimum purchase requirements.

Application Security for Developers

Fed VTE Live! Program—July 12, 2016 at 6:00 am to 10:00 a.m. or July 12 at 11:00 a.m. to 3:00 pm MDT **Two sessions will be held.**

This FREE hands-on course will introduce application developers to basic concepts and practices for ensuring the security of software application against hacker attacks. Students will be given hands-on experience conducting several typical attacks in a simulated coding environment and will discuss possible solutions for mitigating the weaknesses that enable such attacks. Applications must be received prior to June 28, 2016. For more information, contact [Lisa Vasa](#).

MS-ISAC National Webcast Initiative: A Prioritized Approach to Implement the CIS Critical Security Controls

Virtual Event—June 22, 2016 Noon MDT

Implementing the CIS Controls can significantly strengthen security posture. Yet as more organization adopt the controls, many are looking for guidance about how to apply risk management principles in conjunction with the Controls. For insights into ways you can effectively address this challenge, MS-ISAC encourages you to join members of the City of Portland (OR) InfoSec team for a live, case study webcast. [More information and registration.](#)

Incident Response Capabilities in 2016—Parts 1 & 2

Virtual Events—June 8, 2016 11:00 a.m. MDT Part 1: The Current Threat Landscape and Survey Results
June 9, 2016 11:00 a.m. MDT Part 2: Emerging Trends in Incident Response and Survey Results

The third annual SANS survey on incident response will look at the continuing evolution of incident response, how tactics and tools have changed in the last three years, and how security professionals are dealing with increasing numbers and kinds of attacks. The survey report and webcast also will look at key takeaways and recommendation for practitioners and management. [More information and registration.](#)

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

Focus Continued from page 1

other systems from being compromised.

When the device in question is a personal device, disconnect the computer from any network it may be using. Scan the device with anti-malware software with added rootkit detection enabled if available. If infection is found, the most effective remedy is to re-image the device. Many of us are not comfortable with addressing system compromises, including re-imaging our devices. When in doubt, take your device to a trusted technician or repair shop.

This brings up an important point: backup your files! In both the case of a device needing to be re-imaged due to an infection and the case of files being encrypted with ransomware, having a backup of your important files makes the pain of recovery much less. Follow these best practices:

- Do backups regularly. Schedule them to run automatically so you don't forget.
- Backup the files to an external device or an online storage provider.
- Consider making two copies of your backups and store them in separate locations.
- (Note that these backup recommendations apply to your personal devices. Always follow your employer's policies for protecting organizational devices and data.)

Apps and Online Accounts

Many of us are avid users of social media such as Facebook, LinkedIn, Twitter, Instagram, and others. We shop online for everything from clothing to books to auto parts to toys to groceries and every site we use asks us to set up an account. The day may come that you hear of yet another breach. Your password is listed for sale online along with your user ID.

Why should that bother us? Why would anyone want to access my LinkedIn account, for example? Our social media accounts often contain a wealth of information about us as well as our friends and families. In many ways, they are the picture of who we are and a malicious person with access to our accounts can damage our reputation. They may

also use the information to attempt to scam people who care about us.

Perhaps a bigger concern is that too many of us use the same user IDs or email addresses plus the same passwords for multiple accounts. The attacker who has my LinkedIn credentials may guess that the same could be used for Facebook or email. Last month we talked about how access to one account may lead to access to multiple accounts which may lead to the ability to compromise not just personal accounts but work accounts and systems as well.

If you've received notice that an app, account, or service you use has been compromised, change your passwords immediately. If you have not already, enable two factor authentication if available to provide additional security. And if you have used those same credentials for other accounts, change those passwords, too. This time make them unique! It's a good practice to change passwords regularly even if you don't know that an account has been compromised. Too often breaches aren't discovered for months, but if you've made it a habit to change your password by the time it is disclosed you'll already be using a new one.

Financial and Credit Card Accounts

Another area of concern when it comes to account compromise are our financial accounts. The most common ways you'd find out about your financial or credit card accounts being compromised would be having the financial institution notify you of fraudulent transactions or a retailer notifying you of a breach. If you review your statements regularly or, better yet, have set up alerts for activity on your accounts, you may be the one who notices fraudulent activity.

If you do receive notice from a financial institution about a possible compromised account, NEVER give out your full account number, social security number, or other personal information over the phone or via email. Don't click on links in emails without verifying they go to the institution's site. Cyber criminals often use email or the phone to attempt to trick us into providing information to en-

able them to compromise our accounts. When in doubt, contact the institution directly using the number from your previous statements.

Once you've verified that there is fraudulent activity or you've received a notice from a retailer about your account information being disclosed in a data breach, what now? If you are the one who identified the bad transactions, notify your card holder or financial institution immediately. Depending on the type of account, the cards may be cancelled, the account closed and a new one opened for you, and/or other steps taken to remove the fraudulent charges and protect you. In general, credit cards have more legal protections for you than do debit cards, so consider using your debit or bank card as a credit card whenever possible.

If a retailer has notified you of a disclosure, you should also contact your bank or card issuer and request that the card be cancelled and replaced. Criminals sometimes wait months or longer before using or selling card information, so you may be able to prevent fraud by taking action before the activity even occurs. In the case of most data breaches, the entity breached may provide a period of free credit monitoring. Take advantage of those offers and review your credit report regularly. It's not only your money that is at risk. Cyber criminals may also attempt to open new accounts using your information. Activity on these accounts won't get attention like your existing accounts do. You'll find them when reviewing your credit reports or when the criminal doesn't make payments and the creditor tries to collect from you.

Do your part to prevent compromises by updating and patching your devices, protecting your accounts and passwords, and using caution with online activities, but know that it's likely that sooner or later we'll all be victims. By taking steps to backup data, watching for suspicious activity, and knowing how to respond we can react to issues more quickly.

News You Can Use

[Malicious Domain Creation Hits All Time High in Q1 2016](#)

The Infoblox DNS Threat Index set a new record in the first quarter of 2016, driven in large part by a 35-fold increase in ransomware.

[What Does a Corporation Owe You After A Data Breach?](#)

It's a question that grows in importance with each new report of a data breach: How much responsibility should companies take for protecting people's privacy?

[Survey Finds Fears About Privacy and Security Keep People Offline](#)

Concerns about identity theft, financial fraud, and business or government tracking are creating a "chilling effect" on online commerce and free expression.



CAT GOT YOUR TONGUE?!

IF YOU GET AN UNUSUAL EMAIL OR NOTICE YOUR COMPUTER ACTING STRANGELY:

DON'T IGNORE IT, REPORT IT!



Security Quick Tip

Don't fall for the most common scams that are designed to catch your attention:

- ◆ **Shocking news or fake celebrity news!**
- ◆ **Free stuff!**
- ◆ **Urgency!**

Think before you click!

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](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](#)