

Security Matters

Focus on Insiders

It may be hard to imagine, but one of the biggest threats to an organization's security is the people who work there. Security incidents caused by employees are both effective and expensive. But before you start looking at your co-workers with distrustful eyes, let's talk a little bit about insider threats.

These are some of the main insider threats:

- **Malicious attacks**—carried out by employees with either a grudge or a profit motive. This is often what comes to mind when thinking about insiders.
- **Password and information sharing**— providing credentials or information to an unauthorized person, inside or outside the organization, which results in data expo-

sure. The employee may intend to be helpful, but damage still is the result.

- **Accidental exposure** — exposing data by losing an unprotected device or sending a



file to an unintended recipient. The employee does not plan or intend for harm to come from his actions, but sensitive information may fall into the hands of malicious actors.

- **Negligent behavior**—much like accidental exposure, the employee isn't acting intentionally, but instead clicks on a link, downloads or opens a file, or provides confidential information in a social engineering attack.

While many organizations spend 70-80% of their security budgets on keeping the bad guys out, only a small part of their efforts go toward protecting against insiders. That's where you and I come in.

Of the threats discussed above, the malicious insider is the one you're least likely to encounter. That doesn't mean it can't happen in your organization. Research has shown that employees may exhibit warning signs like [Continued on page 4](#)



We all know training budgets are tight and cybersecurity skills are in high demand. One way to address training needs without breaking the bank is using the Federal Virtual Training Environment (FedVTE).

FedVTE is a **free** online, on-demand cybersecurity training system for U.S. government personnel and veterans. FedVTE now has over 100,000 users! Is your organization taking advantage of

this incredible resource?

Managed by DHS, FedVTE contains more than 800 hours of training on topics such as ethical hacking, risk management, and malware analysis. To view the courses available, download the quarterly [FedVTE Course Catalog](#).

Course proficiency ranges from beginner to advanced levels. Several courses help prepare students to take professional certification exams such as Network +, Security +, and Certified Information Systems Security Professional (CISSP).

Did we mention that all this train-

ing is **FREE** for government employees and veterans? All you have to do is sign up for a free account, register for a class, and learn! Get started today by clicking on the button below!

FREE CYBERSECURITY TRAINING

Get trained. Stay trained.
Advance your career.

- 500+ hours of content available
- Certification prep courses
- Beginner to advanced

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	2
Security Training News	3
Training Resources	3
Going For The Gold In Cybersecurity	5
News You Can Use	6



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

Google's July Android security update is its largest ever with patches for 108 different vulnerabilities. The update also introduces a two bundle patch set model to help speed up and provide flexibility in the patching process.

The July 1 patch set address the most urgent vulnerabilities that apply to all Android devices. The July 5 patch set is a "complete security patch level string" which includes the July 1 patches, plus additional items that may not have impact on all Android devices.

Last month **Microsoft** inadvertently reminded the IT community of the need to test Windows system patches before deploying them. June's patches contained security updates designed to fix a vulnerability that could have been used to

mount a privilege escalation attack in the event of a man-in-the-middle attack against traffic flowing between target Windows systems and a domain controller. Unfortunately, the patch broke some organizations' Group Policy Objects (GPOs), causing numerous problems for users.

Microsoft's Sean Greenbaum has since published a blog post on how administrators can repair their GPOs. This is very helpful to those needing to remedy the problems caused by the patch. However, as we always say when sending out security alerts, "apply patches AFTER APPROPRIATE TESTING" and you'll avoid most problems.

Have you or someone in your family caught the **Pokémon Go** bug? Accounts created on iOS erroneously were requesting full permissions on the user's Google account which could have allowed Niantic,

the lead developer of **Pokémon Go** to send and read the user's email and see all of the user's contacts. This issue is now being fixed.

While Niantic is fixing the issue on the client side, this highlights the use of Google accounts and OAuth to authenticate—a protocol that is used throughout the internet. It is worth the time to check what apps you've granted permission to with the Google Security Checkup.

In general, when installing apps, review the permissions the app requests and if they seem intrusive or unnecessary, consider how badly you need the application. There may be an equally good option available which better protects your privacy.

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



Meeting highlights from June 16th, 2016.

Professional Security Training

Lisa Vasa informed the council that the discount buy window for SANS training is open from June 1 to July 31, 2016. Anyone interested in purchasing training or needing more information should contact Lisa.

Policy Assessment Tool pilot

Several agencies are going through the proposed Policy Assessment Tool. Two training sessions have been held for those agencies. The agencies will report on their expe-

riences with the tool at the July 21 meeting.

Best Practices Workgroup

The workgroup finished reviewing the Disposal of Media Storage Devices document and recommended that the Council adopt this document. The Council voted unanimously to do so.

The Council also voted unanimously to adopt the Large Cyber Incident Handling document with several small changes.

The Council discussed the Device Hardening document. The workgroup will continue to update

the document based on comments from the Council and the workgroup. The document will again be on the agenda for the July meeting.

Going forward, the Best Practice and Tools workgroups will be merged into one group, co-chaired by Lynne Pizzini and Dawn Temple.

Situational Awareness Workgroup

Bryan Costigan mentioned that the Situational Awareness Workgroup met to discuss its way ahead, given that both of its current items have been rolled into the Best Practices Workgroup.

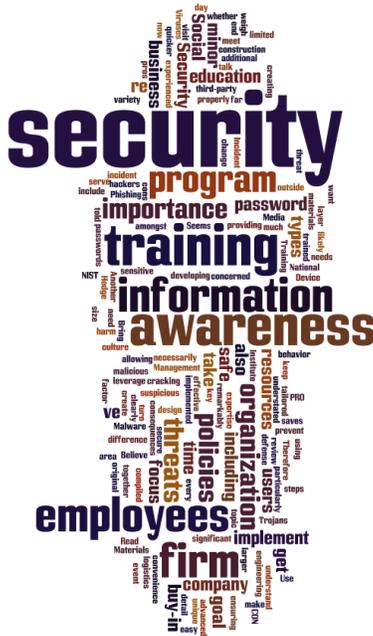
Other Discussion

There is an opportunity to participate in a tabletop exercise with the Department of Homeland Security. The tabletop exercises will be held September 13, 14, and 15. It is a four-hour cyber-based exercise facilitated by DHS. Contact Lynne Pizzini for more information.

Next Meeting

The next meeting of the MT-ISAC will be held Thursday, July 21, 2016 from 11:00 a.m. to 1:00 p.m. at the Capitol, room 137.

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.

OnGuardOnline has moved. This great site for free online security tips and resources has move to the Federal Trade Commission’s website. Update your Favorites and share with friends, family, and co-workers. <https://www.consumer.ftc.gov/features/feature-0038-onguardonline>

Become a NCSAM Champion. The National Cyber Security Awareness Month (NCSAM) Champion program is a way for organizations to officially show support. Being a Champion is easy and does not require any financial support. NCSAM Champions receive a toolkit that includes a wide variety of resources, such as sample social media content, recommendations for getting involved at work, and a press release template to help promote the month. More information is available on the [StaySafeOnline](#) site.

Ransomware & Malvertising: Dominating the Threat Landscape

Virtual Event—July 14, 2016 at 1 p.m. MDT

Better understand the impact of malvertising and ransomware. Learn some of the biggest misconceptions, and see how these attacks are delivered and why your organization may be at risk—without you even knowing it. [More information and registration.](#)

The State of Cyber Threat Intelligence — Parts 1 & 2

Virtual Events—August 16, 2016 11:00 a.m. MDT Part 1: How Cyber Threat Intelligence Is Consumed and Processed
August 17, 2016 11:00 a.m. MDT Part 2: Emerging Trends in Incident Response and Survey Results

The second annual SANS survey on cyber threat intelligence will look how the IT community gather and consume cyber threat intelligence (CTI) and do their CTI implementations provide value. [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

frequent absences, changes in temperament, unusual behavior such as suddenly working late or coming in early, attempts to access restricted areas or systems, or making unauthorized changes to systems. Note that there may

be many legitimate reasons for these signs, but if something seems suspicious or “off”, report it.

If you are a system administrator, be sure that you have procedures in place to log and review unauthorized access attempts as well as all system configuration changes—even those by authorized administrators.

From an organizational point of view, keep in mind that the majority of insider attacks happen after an employee leaves. Processes to insure that all access is disabled or removed when an employee resigns or is terminated are a must. It’s also important to promptly change any administrative passwords to which the employee may have had access.

When it comes to password and information sharing, the first step to just say no. Administrative passwords are especially prone to sharing with one survey finding that 52% of IT staff have shared credentials with a co-worker and 59% have shared them with a contractor.

While it’s tempting to be helpful with a co-worker or a vendor needs access to “get things done”, your organization should have procedures in place to grant access to those who truly need it whether it’s normal or emergency access. Savvy cybercriminals have learned one of the easiest ways to gain access is to simply ask.

Policies and procedures, while good, can only go so far in preventing accidental exposure of private information. Employees need to know and understand organizational policies regarding the use of mobile devices such as laptops, tablets and smart phones as well as procedures for properly storing and transmitting information. Still, accidents can happen. A laptop may be stolen from a parked car. A smart phone may be left at the airport. A mistake in an email address may send a file to an unauthorized recipient.

All mobile devices should be protected by strong passcodes or passwords and two-

factor authentication when possible. Device encryption is also recommended. Mobile Device Management (MDM) software can also provide tools to remotely wipe organizational data in the event a device is lost or stolen. Of course, keeping a close eye on your mobile devices is always the first step to preventing loss.

When handling sensitive files, make sure you understand who should and should not have access to them. Use care when sending them to others or storing them to ensure they are not accessible by unauthorized people. Double check the email address before clicking send. When working with the files, be aware of what others may be able to see on your desk or computer monitor and take steps to prevent unauthorized exposure.

Using due care is a key to avoiding becoming an insider threat yourself. We don’t intend to expose sensitive information, but falling for phishing and social engineering attacks or improperly handling and disposing of documents may make us unwitting accomplices in the exposure of information to unauthorized people. Here are some tips to help avoid that:

- If it looks or sounds too good to be true, it probably is.
- Think before you click. Check hyperlinks to see what site they open and carefully examine emails. Phishing is becoming more and more sophisticated

- Always follow your organizations procedures for visitors or maintenance personnel. Don’t be afraid to ask questions when you see strangers in your workspace.
- Don’t fall for requests for “emergency” access or when someone say “just this once can you help me out”. Always follow procedures for granting access and providing information.
- If you use a mobile device for work, use strong passwords and two factor authentication when possible. When you’re traveling, keep your device in sight at all times. Even when just going from work to home with a device, don’t leave it in your car for someone to steal.
- When handling printed documents, lock them in a cabinet or your desk when they are not in use. Shred them or put them in locked shred bins when you no longer need to retain them.



Going For Gold In Cybersecurity

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

The world's attention will turn to Rio de Janeiro this summer as Brazil will be the first South American venue to host the Olympic Games. This sporting event is sure to generate a vast amount of popular interest with both fans and media alike and this kind of attention holds potential value for those looking to prey upon the attraction of the games to perpetrate cyber fraud schemes.

Make sure it's official

The international interest in the Olympic Games, the variety of sports, and the seventeen-day schedule makes for a lengthy window of opportunity for criminals to take advantage of. Fraudsters have the luxury of time and a variety of interest areas to choose from in trying out their schemes to see what works and then to improve upon the effectiveness. How can you avoid being a victim of these schemes? The simplest way is to be cautious and to understand the fraud schemes that you can expect to encounter.

We know that the criminals have already begun trying to entice victims with the lure of false tickets. This type of activity is likely to continue to be targeted to tourist audiences who are in the market to purchase event tickets. To avoid being scammed, only use the official site of the [Olympics Games](#) to find the official ticket vendor, the official vendor for the U.S. is [CoSport](#). Criminals are creating very sophisticated, look-a-like sites, which are difficult to discern from official ticketing sites. These false sites even mimic expected customer service responses to delay the reporting of the theft.

Be aware

We also know that ransomware is currently one of the most popular criminal methods and is sure to be used in conjunction with enticing Olympics-themed email messages. What is [ransomware](#)? Ransomware infections may encrypt files on a victim's computer and demand a ransom be paid to allow the victim to regain access to the files. Malvertising is one of the most common gateways for malicious software to be installed on a device. Malvertising, or malicious advertising, is the use of online, malicious advertisements to spread malware and compromise systems. The advertisement, or email and its attachment will be carefully designed to draw upon your interest in the hope of getting you to open them. You can learn to [spot these messages](#) by being mindful, being observant, and being aware of attachments.

The fraudulent messaging around the Olympics will look identical to what you would expect to receive from a sales or promotion around these games. Do not respond to, or click links in unsolicited emails. If you are interested in an offer being advertised, a safer alternative is to use a search engine to find the official vendor's site and to visit it directly to look for the offer. If the deal is available, then it is likely going to be promoted on the vendor's website. Fraudsters may also use other attention-getters surrounding the Olympic games, such as "Zika outbreak at the Olympics!"

The Rio Olympics will begin on August 5 and last until August 21, with more than 10,000 athletes competing in 306 events. Careful attention to the sites that you visit for your Olympics purchases or to watch the games online will make them more enjoyable. Go Team USA!

Recommendations

- ◆ Do not visit untrusted websites or follow links provided by unknown or untrusted sources.
- ◆ Do not open attachments from unknown or untrusted emails.
- ◆ Use up-to-date anti-virus.
- ◆ Patch all systems and applications.

One of the early schemes targeting interest in the 2016 Olympics occurred approximately one year ago, just as the Olympic ticket market was taking shape. The fraudsters sent out false messages purporting to be from the Brazilian government and the International Olympic Committee (IOC) claiming that recipients had won a ticket lottery. All one had to do was provide the criminal with banking or personal information. This information was then used to steal money from the individual.

Provided By:



The information provided in the Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.

News You Can Use

[Insider Data Theft & Malware Infections Among Biggest Threat in 2016](#)

Insider data theft and malware attacks top the list of the most significant concerns for enterprise security executives, a new report from Accenture and HFS Research finds.

[Ruling Could Make Password Sharing Illegal](#)

If you need more reasons to not share your password, a new federal court ruling could make sharing your passwords for subscription services a federal crime.

[Phishing, Whaling, & The Surprising Importance of Privileged Users](#)

By bagging a privileged user early on, attackers can move from entry point to mission accomplished in no time at all.



Security Quick Tip

Trust Nobody!

If you receive a gift, find a USB drive, or are asked to perform a command on your computer, ask "Why?" or "Do I know the person who's asking me this?" Don't be afraid to decline or ask for more information. Exactly like we teach our children: Don't talk to strangers!

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



[Enterprise Security Program](#)

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

[Joe Frohlich, Enterprise Security Manager](#)