

Security Matters

Focus on Email

For many of us it's hard to imagine a day without email. Whether we're at home or at work, there always seems to be a new message waiting in our email. Email provides an efficient way to share information, stay informed, and communicate with co-workers, friends, and family. But dangers may be mixed in with legitimate messages.

More than likely you know about phishing – email-based attacks that seek to trick you into taking actions that will compromise your accounts, provide user IDs and passwords, or infect your devices. Phishing is one of the most commonly used and effective attacks used by cyber criminals. While phishing, spear-phishing (targeting a group of individuals based on employer, job, or other characteristic), and whaling (targeting high value individuals like CEOs) are becoming more and more sophisticated, staying aware can go a long way toward keeping you safe. For example:

- ◆ Do you know the person or recognize the originating email address?
- ◆ Pay attention to spelling and grammar. Cyber-criminals sometimes have poor spelling or grammar.
- ◆ If the message says you must take action immediately or face dire consequences, that may be a sign that the message is a trick.
- ◆ Watch for 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.



- ◆ Beware of links in email. If you see a link in a suspicious email message, don't click on it.
 - ◆ Cyber-criminals often use threats that your security or account has been compromised.
- If the email contains a link hover your mouse over it to verify where the link goes. Alternately, you can open a browser and manually type in the site URL if it is a link from an organization with which you have a relationship. [Continued on page 5](#)

When presented with what might be a phishing email, review the sender's email address. Is it someone you know and does the address, not just the name, appear to be from a legitimate sender?

World Password Day 2016

May 5th was World Password Day. According to the National Cyber Security Alliance (NCSA), "Email accounts in particular are extremely important to protect as once breached, hackers can use them to reset passwords and break into other accounts, steal identities, target contacts and put an individuals' reputations at risk."

● **Create strong passwords.** Use a combination of at least 12 upper and lower case letters, numbers, and special characters. Passphrases make it easier to remember complex passwords.

- **Get two steps ahead and protect core accounts** – such as email, financial services, and social networks – with multi-factor authentication. Multi-factor authentication requires a second step, such as a text message to a phone or the swipe of a finger to be used in addition to a password to log on to an account.
- **Use unique passwords for each account.** You wouldn't use the same keys for your car, your office, and your home would you? Passwords are like keys to your digital life. Don't make it

easy for criminals by using the same one for everything.

- **Use a password manager.** Password manager can keep track of or even generate strong passwords for you. You only have to remember one strong master password. Many of the managers available today restrict use to devices you've registered which further protects your passwords.

For some other advice, let Betty White give you a pep talk in four different videos: <https://passwordday.org/>

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	2
Security Training News	3
Training Resources	3
Awareness Event Prize Winners	3
News You Can Use	5



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

This is the ninth year Verizon has published its annual Data Breach Investigations Report (DBIR). The report used 64,199 security incidents and 2,260 data breaches to analyze patterns, trends, and items of interest to those who are seeking to understand and prevent security incidents. The full report is available for download [here](#). Below are some main takeaways from this year's report.

The first takeaway from the 2016 DBIR is that there is no industry, area, or organization that is safe from compromise. Among the industries most affected by data breaches were financial, retail, accommodation, information, and public sectors. Most of the attackers were external actors motivated by financial gain.

As for how cybercriminals attack, phishing and point-of-sale (POS) compromise are the most likely tools used for successful attacks. For all phishing campaigns in 2015, some 30% of messages were opened by the intended target with 12% of those target clicking on the link or attachment.

The acquisition of credentials play a larger part this year compared to the past, giving attackers an easier route to reaching their goals. According to the DBIR, 63% of confirmed breaches used weak or stolen passwords. Phishing and web-based mail servers were the source of many of the stolen credentials.

The DBIR also discusses the increased time to discovering compromises. Not only is the time to discovery getting worse, but that discovery is least likely to be made

by internal parties. Instead, law enforcement, third parties, and fraud detection mechanisms usually detect the problem first. A more promising note is that incidents are being discovered more quickly overall.

Also noted in the report is that attacks often are multi-staged. No longer is the attacker satisfied with compromising a system and taking what he came for. Instead, the attacker may use information from one attack to target more sensitive systems or another set of victims.

The DBIR is interesting reading with a number of insights and recommendations for preventing incidents. It's worth spending some time reading the full report.

Security Awareness 2016 Events

Focus on Passwords

- ◆ May 24, 2016 - 2:30—4:30 at the Metcalf Building, Conference Room 111
1520 E. 6th Ave



Check [Montana Information Security](#) for the latest event schedule and contact [Lisa Vasa](#) if you'd like to host an event.

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



Time Change for MT-ISAC Meetings – The MT-ISAC Council has approved to move the meeting time to 11AM to 1PM. This time change will start with the upcoming May 19th meeting and continue for future meetings. The MT-ISAC will still continue to meet the 3rd Thursday each month.

MT-ISAC Review – There was a discussion and review of the MT-ISAC goals and objectives. The discussion was around a document called the “Workgroup List” that has been posted to the MT-ISAC website with the April 21st meeting items. If you are curious on what has taken place within the MT-

ISAC and its workgroups this would give a high level overview.

Technical Small Cyber Incident Handling Steps – Best Practices workgroup is finalizing Council recommendations and will soon be posted final draft for approval of council. For more information please see the website.

Assessment Pilot Program – DOA, DOR as well as other agencies will conduct a pilot on filling out the Assessment document. The pilot will help determine the effectiveness of using the assessment document and the time involvement needed. To obtain a copy please see the website.

Focus [Continued from page 1](#)

Be cautious opening attachments as well. If you don't expect an attachment – even when it appears to be from a friend – contact the sender and verify it.

Phishing isn't the only danger connected to your email accounts, however. I recently posted an article about email accounts and passwords being breached and was asked, "why would anyone care about my email?"

For work email, that answer would seem obvious: some of us handle confidential information that is protected by law. Others may not have that level of information to protect, but the contents of a message may not be something they'd want to share with the world at that time. For those who work in government, email is subject to disclosure laws, so we could argue that it's public anyway. However, even in those circumstances, email may be sensitive at the time it is sent but not later or may be exempt from disclosure.

Our personal email is less likely to contain protected personal identifiable information (PII) about others and most people would say that it rarely contains PII about ourselves. I'd suggest that we stop and think for a moment about all the things we use email for today. For example, more and more organizations are encouraging customers to receive documents and notifications via email. Online shopping is common, with purchase confirmations and shipping notifications arriving via email. Our medical care providers send us

reminders about appointments and lab reports. We pay bills online with statement and payment notices being sent to our email. In this day of data breaches, we sign up for credit and identity monitoring and reports are sent to our email. Our email addresses are associated with our social media accounts. Then there are all the accounts simply for accessing sites' content. It's not hard to have our email address associated with many accounts – some we don't even remember!

What do you do if you forget the password to one of those accounts? For most, you request a new password or a link for resetting your password be sent to – you guessed it – your email address. This works on the assumption that you alone have access to your email, so you are the only one who can view or reset your password using the email. But what if your email account is compromised? Now a cyber-criminal can look through emails to see what accounts you might have. He can go to those accounts and request passwords or resets and with access to your email, change them. He can even change the email address associated with the account to something he controls, not you.

Fortunately, most of our most sensitive accounts have additional controls like PINs or security questions so the password alone isn't enough to access our bank accounts. But, the determined cyber-criminal has gained valuable information about you and your passwords. Many people use the same passwords for multiple accounts despite that being a bad practice. Others use similar pass-

words for each site and if the cyber-criminal is able to determine several of those passwords, he may be able to figure out the pattern, thus gaining access to others. Throw in the availability of personal information on social media and he may also have clues to your PIN or security questions if they are related to your personal information. It's not your email contents he wants – access to more valuable accounts is his goal.

Cyber-criminals often used spoofing to try to fool users into believing email is sent from someone they know. Checking the sender's actual email address in the message can detect senders who are only pretending to be someone. When an attacker has control of your email account, he can not only pretend to be you, he IS you as far as the address on the email is concerned. He can leverage that account to do more mischief with your friends—even the ones who are careful to check addresses on suspicious emails. He can also potentially use your relationship with people in your contacts list to gain more information and access.

What should we do to protect our email and our other accounts?

- Use two-factor authentication for your accounts. Not sure if it's available for your accounts? Visit <https://www.turnon2fa.com/> to check.
- Change your passwords regularly and use unique passwords for each account.
- Consider signing up for a free email account to use for site registrations rather than using your primary email account.
- Keep your inbox cleaned up so if it compromised there are few clues to other accounts you may have.
- If you see a notice about a password reset in your email and you didn't request the reset, notify the company immediately and change the password again yourself.
- Consider using encrypting your email when possible to add security.

We take for granted the convenience and availability of information and services through email, but we should never ignore the risks that come with that convenience and availability. Watch for attacks in your inbox and manage your account with the same precautions you'd use for other sensitive accounts and PII. And when you read or hear news that millions of email accounts have been hacked, don't just shrug and say, "why would anyone want my email?"



News You Can Use

[The Giant Email Hack That Wasn't](#)

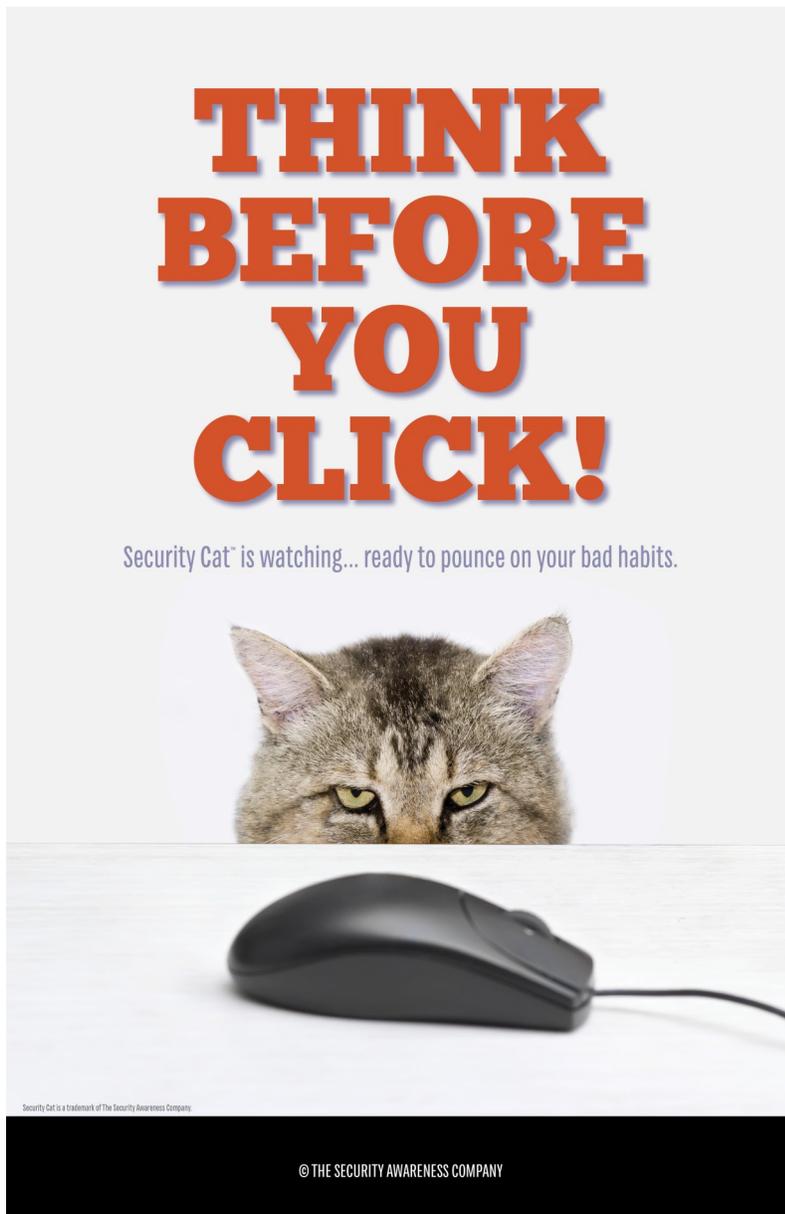
On Thursday, a Reuters report described how hackers were peddling some 272.3 million usernames and passwords for unsuspecting users' email accounts, raising concerns of yet another major data breach at a time when cybersecurity sensitivity is at an all-time high. By Friday, though, the services themselves (as well as independent analysts) concluded that the situation was not quite what it seemed.

[Email Hack At Troy Business Results in \\$500,000 Wire Transfer to Hong Kong](#)

Police report an employee at a Troy business was duped into sending nearly \$500,000 to a bank in Hong Kong.

[Advanced Cybercriminals Target You As An Individual](#)

Each time we hear of a phishing scam, we tend to believe that it would never happen to us.



Security Quick Tip

If you get an email from your bank or other service (bill payments, credit monitoring company, etc.), always visit the website manually. No copy and paste. No direct clicking. You'll thank yourself later.

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](#)