



IT Security Update

Board of Regents, February 20, 2014

Karl Kowalski, Chief Information Technology Officer



National Data Privacy Month

February 2014

Data Privacy Month (DPM) is an annual effort to empower people to protect their privacy and control their digital footprint and make protection of privacy and data everyone's priority.

Common Ways Privacy is Compromised:

Spam -- Spam is the electronic equivalent of junk mail. The term refers to unsolicited, bulk – and often unwanted – email.



Phishing -- Phishing attacks use email or malicious websites (clicking on a link) to collect personal and financial information or infect your machine with malware and viruses.

Spear Phishing -- Spear phishing is highly specialized attacks against a specific target or small group of targets to collect information of gain access to systems





DON'T GET HOOKED!

WHAT IS PHISHING?

Phishing is a psychological attack used by cyber criminals to trick you into giving up information or taking an action. Phishing originally described email attacks that would steal your online username and password. However, the term has evolved and now refers to almost any message-based attack. These attacks begin with a cyber criminal sending a message pretending to be from someone or something you know, such as a friend, your bank or a well-known store.

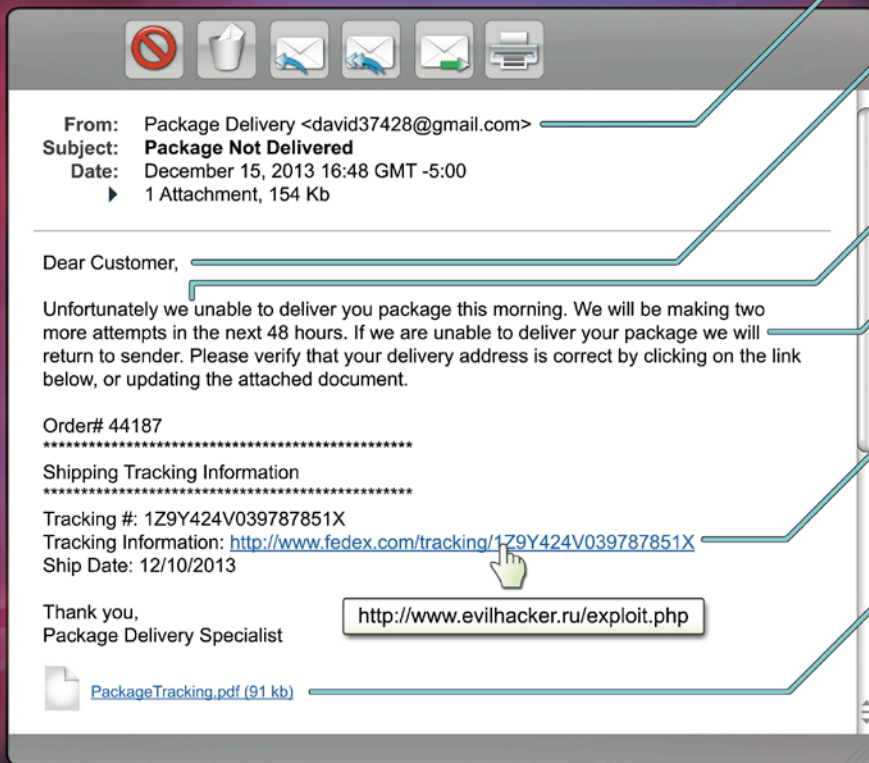
These messages then entice you into taking an action, such as clicking on a malicious link, opening an infected attachment, or responding to a scam. Cyber criminals craft these convincing-looking emails and send them to millions of people around the world. The criminals do not know who will fall victim, they simply know that the more emails they send out, the more people they will have the opportunity to hack. In addition, cyber criminals are not limited to just email but will use other methods, such as instant messaging or social media posts.

WHAT IS SPEAR PHISHING?

The concept is the same as phishing, except that instead of sending random emails to millions of potential victims, cyber attackers send targeted messages to a very few select individuals. With spear phishing, the cyber attackers research their intended targets, such as by reading the intended victims' LinkedIn or Facebook accounts or any messages they posted on public blogs or forums. Based on this research, the attackers then create a highly customized email that appears relevant to the intended targets. This way, the individuals are far more likely to fall victim.

WHY SHOULD I CARE?

You may not realize it, but you are a phishing target at work and at home. You and your devices are worth a tremendous amount of money to cyber criminals, and they will do anything they can to hack them. YOU are the most effective way to detect and stop phishing. If you identify an email you think is a phishing attack, or you are concerned you may have fallen victim, contact your help desk or security team immediately. To learn more about phishing or to demo the SANS Securing The Human phishing testing platform, please visit <http://www.securingthehuman.org/phishing>.



PHISHING INDICATORS

- A** Check the email addresses. If the email appears to come from a legitimate organization, but the "FROM" address is someone's personal account, such as @gmail.com or @hotmail.com, this is most likely an attack. Also, check the "TO" and "CC" fields. Is the email being sent to people you do not know or do not work with?
- B** Be suspicious of emails addressed to "Dear Customer" or that use some other generic salutation. If a trusted organization has a need to contact you, they should know your name and information. Also ask yourself, am I expecting an email from this company?
- C** Be suspicious of grammar or spelling mistakes; most businesses proofread their messages carefully before sending them.
- D** Be suspicious of any email that requires "immediate action" or creates a sense of urgency. This is a common technique to rush people into making a mistake. Also, legitimate organizations will not ask you for your personal information.
- E** Be careful with links, and only click on those that you are expecting. Also, hover your mouse over the link. This shows you the true destination of where you would go if you clicked on it. If the true destination is different then what is shown in the email, this is an indication of an attack.
- F** Be suspicious of attachments. Only click on those you are expecting.
- G** Be suspicious of any message that sounds too good to be true. (No, you did not just win the lottery.)
- H** Just because you got an email from your friend does not mean they sent it. Your friend's computer may have been infected or their account may be compromised. If you get a suspicious email from a trusted friend or colleague, call them on the phone.

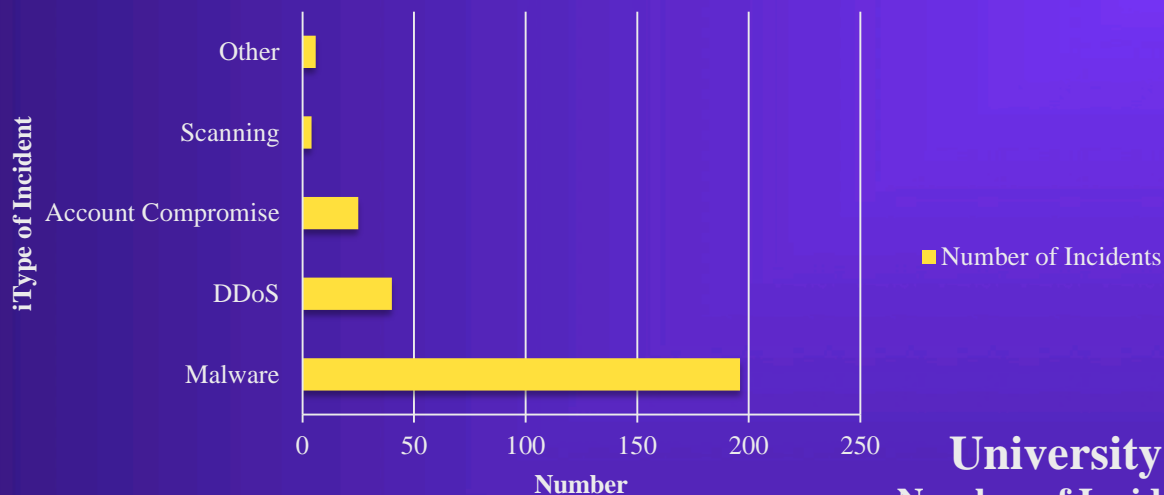
This poster was developed as a community project. Contributors include: Cheryl Conley (Lockheed Martin), Tim Harwood (BP), Tonia Dudley (Honeywell), Ellen Powers (MITRE Corporation), Shanah Johnson (Reserve Bank of Atlanta) and Terri Chihota.

Corporate Compromises 2013

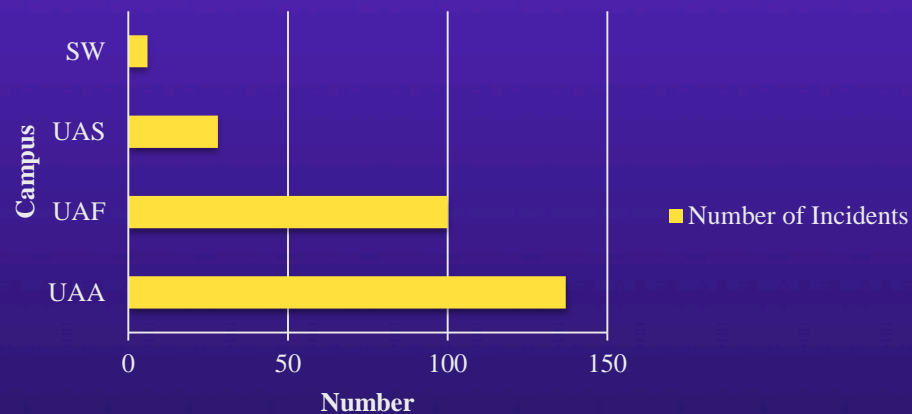
- Target 110,000,000 records
- Michaels (unknown)
- Neiman Marcus 1,100,000 records
- Veteran's Affairs eBenefits 5,000 individuals
- Coca-Cola 74,000 individuals

UA Incident Distribution 2013

University of Alaska
Number of Incidents by Type
January-December 2013

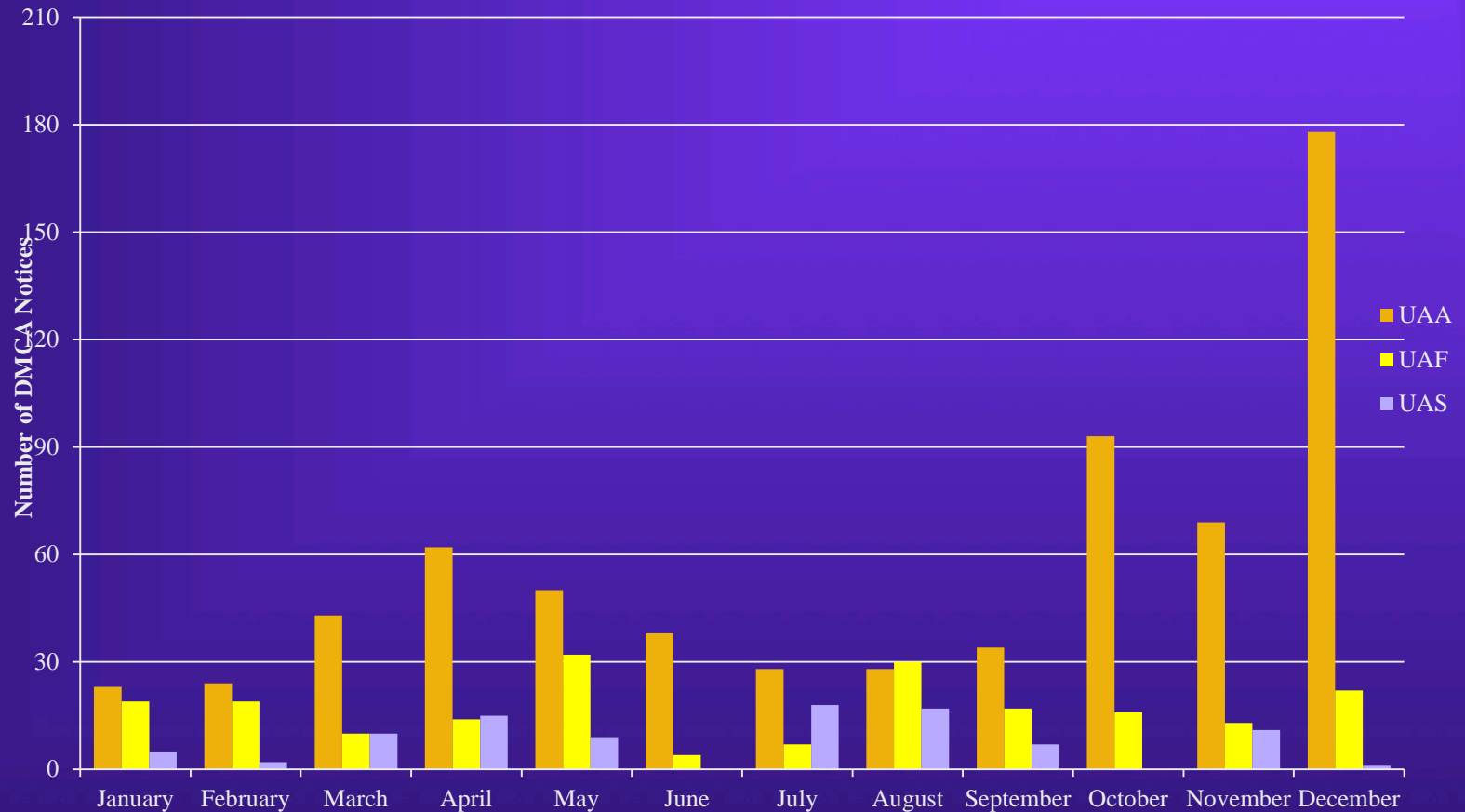


University of Alaska
Number of Incidents by Campus
January-December 2013



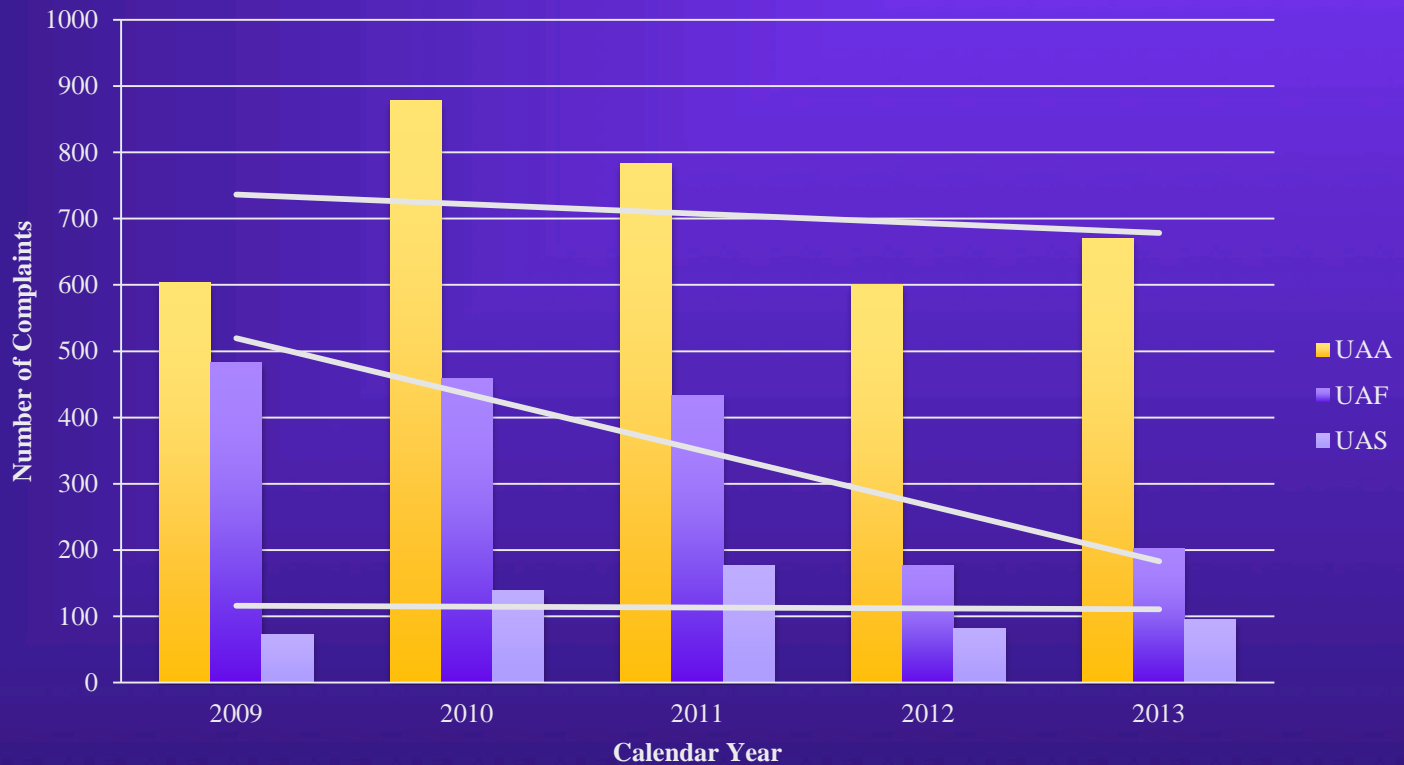
Copyright Complaints

University of Alaska
Copyright Complaints Received
2013



Copyright Complaints

University of Alaska
Copyright Complaints
2009-2013





UAA DMCA Compliance Coordination Effort

- Prior to 2013 minimal effort was made to identify copyright infringers at UAA
- Pat Shier, CIO & Adam Paulick made enabling the infrastructure to identify infringers on the network a priority
- UAA ITS worked with OIT Security to establish necessary logging and access for OIT's current investigator to validate complaints
- As of January 2014 the ability to identify infringers on UAA managed networks is in place and investigation is done by OIT Security
- UAA ITS follows up locally with individuals, the Dean of Students and/or HR as appropriate to address the behavior
- We hope to reproduce the reduction in complaints and recidivism we have seen at UAF and UAS in the coming years



Final Note

Protect Yourself with these STOP. THINK. CONNECT. Tips:

Keep a Clean Machine: Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.

When in doubt, throw it out: Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.

Protect all devices that connect to the Internet: Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.

Plug & scan: "USBs" and other external devices can be infected by viruses and malware. Use your security software to scan them.



Resources

- <http://www.staysafeonline.org/>
- <http://www.securingthehuman.org/>
- <http://ist.mit.edu/security/tips>
- http://www.fbi.gov/scams-safety/computer_protect
- <http://www.dhs.gov/stopthinkconnect>