

THE SOCIAL MENACE

SOCIAL MEDIA AND ITS IMPACT ON SENSITIVE DATA

State of Maine



Luke Emrich, Supervisor, Security and Privacy Services, RSM US LLP

Presenter info

Luke Emrich

Supervisor, Security and Privacy Services

5+ years experience in:

- Computer forensics
- Incident response
- Malware analysis
- Litigation response (e-discovery) Yuck*



RSM US LLP

Boston, Massachusetts

luke.emrich@rsmus.com

+1 315 534 9556



Agenda

- RSM's security and privacy services
- The cyber threat landscape
- Security threat scenarios
- Social media
- Attackers + social media = trouble
- What can be done
- Questions

RSM'S SECURITY AND PRIVACY SERVICES



Security and privacy services

RAS consulting

Security Governance

- Management and frameworks (ISO, NIST, HIPAA, etc.)
- State, federal, international regulations

Security Testing

- “On the keyboard” i.e., ethical hacking
- Penetration testing
- Vulnerability assessments

PCI

- PCI DSS assessments/gap analysis
- Approved scanning vendor
- Review of payment applications

Digital Forensics and Incident Response (DFIR)

- Investigative Support
- Incident response
- Real time threat detection and malware analysis.

Security Architecture

- Process integration
- Vendor selection
- Performance improvement / Architecture design

THE CYBER THREAT LANDSCAPE

Misconceptions and Attack Vectors





“The world isn’t run by weapons anymore, or energy, or money. It’s run by little ones and zeroes, little bits of data. It's all just electrons.”

Cosmo - Sneakers

Before we go any further *Definitions... “the hacker” versus “the attacker”*

hack·er noun \ 'ha-kər \

- A technologically savvy person, good at finding weaknesses in complex systems
- Two ways to describes hackers depending on how they use their skills
 - White Hat (Used by “good” guys)
 - Black Hat (Used by “bad” guys)

White Hat methods means using technical skills with permission of system owners and with the goal of fixing any weaknesses



at·tack·er noun \ ə 'takər \

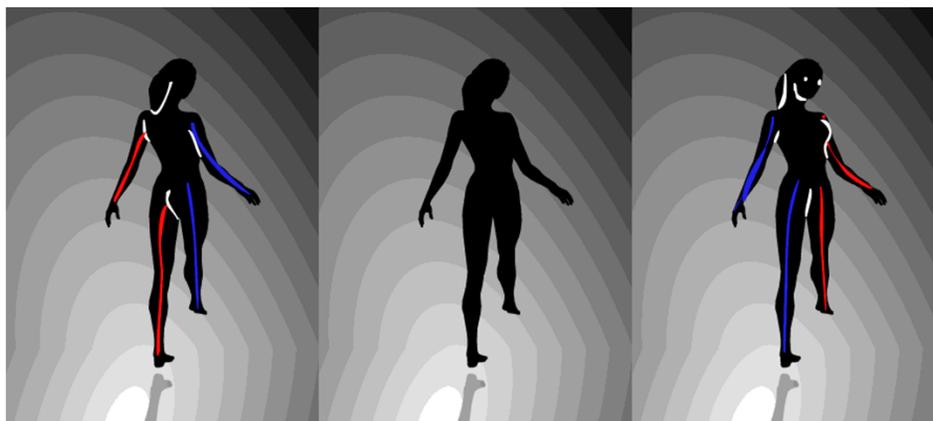
- A hacker who uses Black Hat methods, which means using their skills to find and exploit weaknesses for financial gain, or personal and/or ideological reasons
- These are the guys that:
 - Infect computers with malware, trojans or viruses
 - Breach security systems to steal or destroy data
 - Steal identities and commit fraud
 - Engage in phishing
 - Carry out denial-of-service attacks
 - Steal intellectual property



Security misconceptions

The attackers are not exactly who you think they are

- Many of the standard methods of protection are now being bypassed with ease
- The underground economy has lowered the knowledge threshold
- Skilled attackers make more money at less risk by selling their knowledge in packaged form : Kits, automation, subscriptions, malware pre-packs, etc.
- Result: Pseudo “APT” attackers
 - Advanced Persistent Threats
 - a.k.a “Idiots with nuclear weapons”
- Result: Attackers have moved from brute force to simplicity, misdirection, abuse of trust



The more we see the less we know



Security statistics

Three most prevalent attack vectors

- Social engineering (phishing for credentials and more)
 - Why bother to do all the heavy lifting involved with “hacking” when you can just ask someone to do something for you?
 - While there is a technical component, the attack is against human nature
- Malware (keyloggers, ram scrapers)
 - Finding and purchasing nondetectable malware in the underground market is trivial
 - Modern anti-virus is an 80–20 proposition at best
- Hacking
 - “Traditional” hacking is used post-breach, not as the original entry point
 - Current methods focus on web apps and browser plugins

SECURITY THREAT SCENARIO

Recon—Social Engineering—Attack—Payday



Recon and social engineering

- Recon:
 - What is a potential target advertising or broadcasting?
- Social engineering: Fancy name for traditional “con games”
 - Attacking an environment via manipulating people
 - Focused on user habits, mannerisms, human nature, entrenched organizational procedures and activities
- Hacking by the KISS principle
 - Keep it simple, stupid
- Why go through all of the effort to bypass firewalls, anti-virus, monitoring solutions, etc.?
- Why not just have the target do all the work for you?



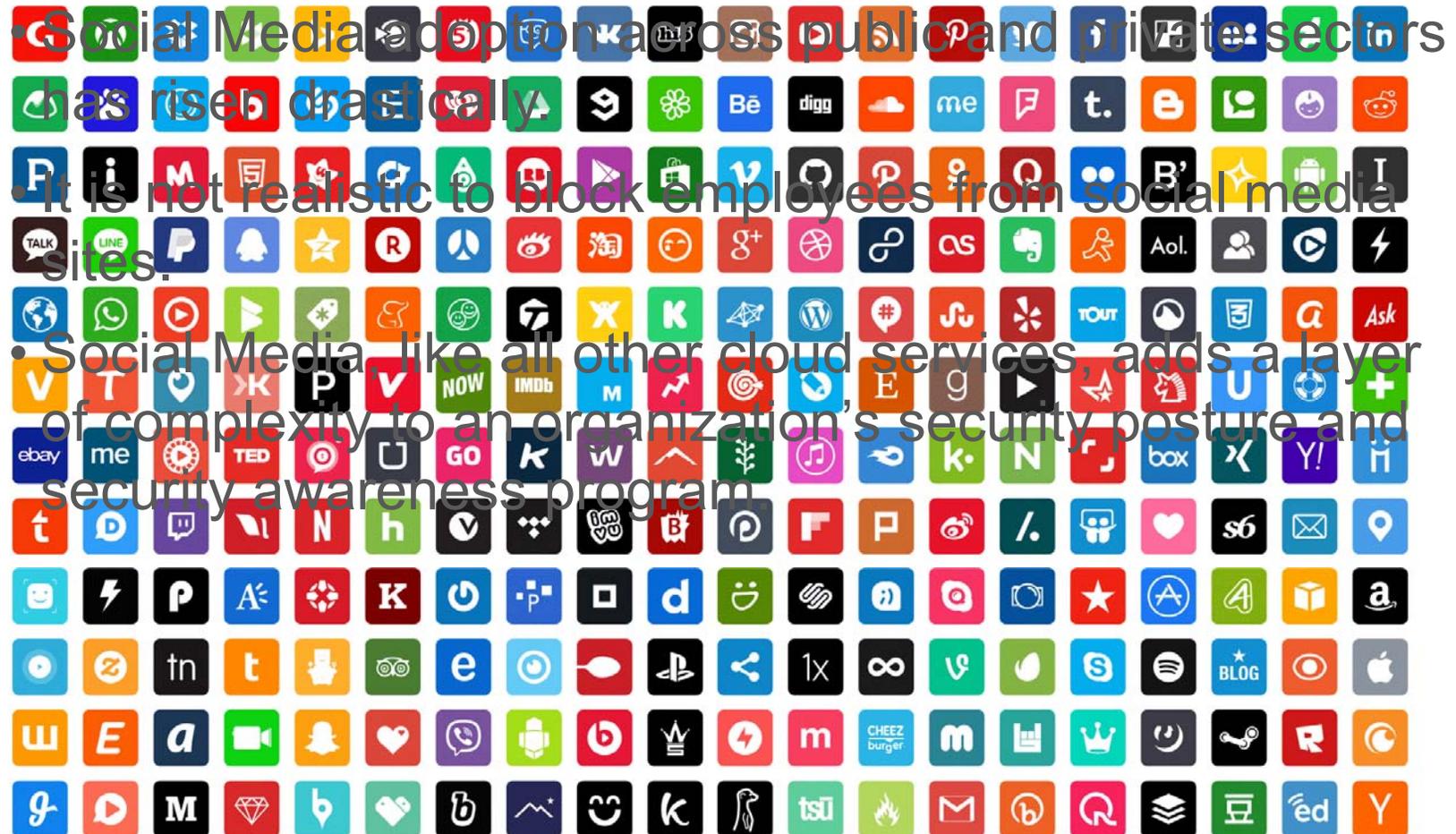
SOCIAL MEDIA

Misconceptions and Attack Vectors



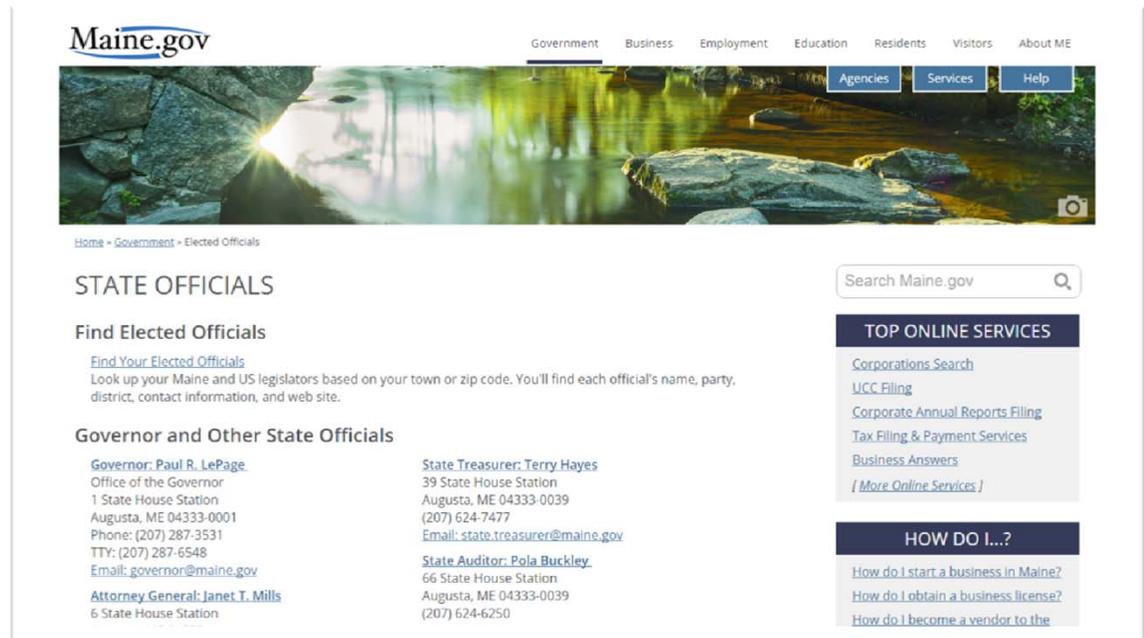
Social media

Yeah, it's huge...



Recon—social media

- Corporate website
 - Org chart(s)
 - Employee information
 - Title
 - Phone number
 - Email address
 - Roles/bio



The screenshot shows the Maine.gov website. The header includes the Maine.gov logo and navigation links for Government, Business, Employment, Education, Residents, Visitors, and About ME. Below the header is a large banner image of a river with a person's face reflected in the water. A search bar is located in the top right corner. The main content area is titled "STATE OFFICIALS" and includes a section for "Find Elected Officials" with a link to "Find Your Elected Officials". Below this is a section for "Governor and Other State Officials" listing the Governor, State Treasurer, and State Auditor with their contact information. On the right side, there are two boxes: "TOP ONLINE SERVICES" with links for Corporations Search, UCC Filing, Corporate Annual Reports Filing, Tax Filing & Payment Services, and Business Answers; and "HOW DO I...?" with links for How do I start a business in Maine?, How do I obtain a business license?, and How do I become a vendor to the state.

Recon—social media (cont.)

- LinkedIn—Business Presence

- Current and past employment
- Contact information
- Education
- Skill sets
- Roles/bio
- Colleagues
- Interests
- Common connections
- Physical characteristics

The screenshot shows a LinkedIn profile for Terry Hayes, Treasurer at State of Maine. The profile includes a profile picture, a header with the name and title, and a 'Send Terry InMail' button. The background section is titled 'Summary' and contains the text: 'I thrive on collaborating with people from across Maine to expand the quality of life for all of us who are fortunate enough to live and work here.' Below the summary is a document icon and the text 'Maine Legislature to join Maine Employers In...'. The right sidebar features a 'People Also Viewed' section with profiles of Kristi Carlow, Neria Douglass, Richard Bennett, Jillean Long Battle, and Kelly Mitchell. There is also a Toyota advertisement for a Highlander photo gallery.

Recon—social media (cont.)

- Facebook—Personal presence

- Contact information
- Education/work
- Family/friends/relationships
- Current/previous residences
- Interests
- Connections to organizations and/or beliefs
- Physical characteristics
- Good/Bad/Ugly



ATTACKERS + SOCIAL MEDIA = TROUBLE

Putting It All Together



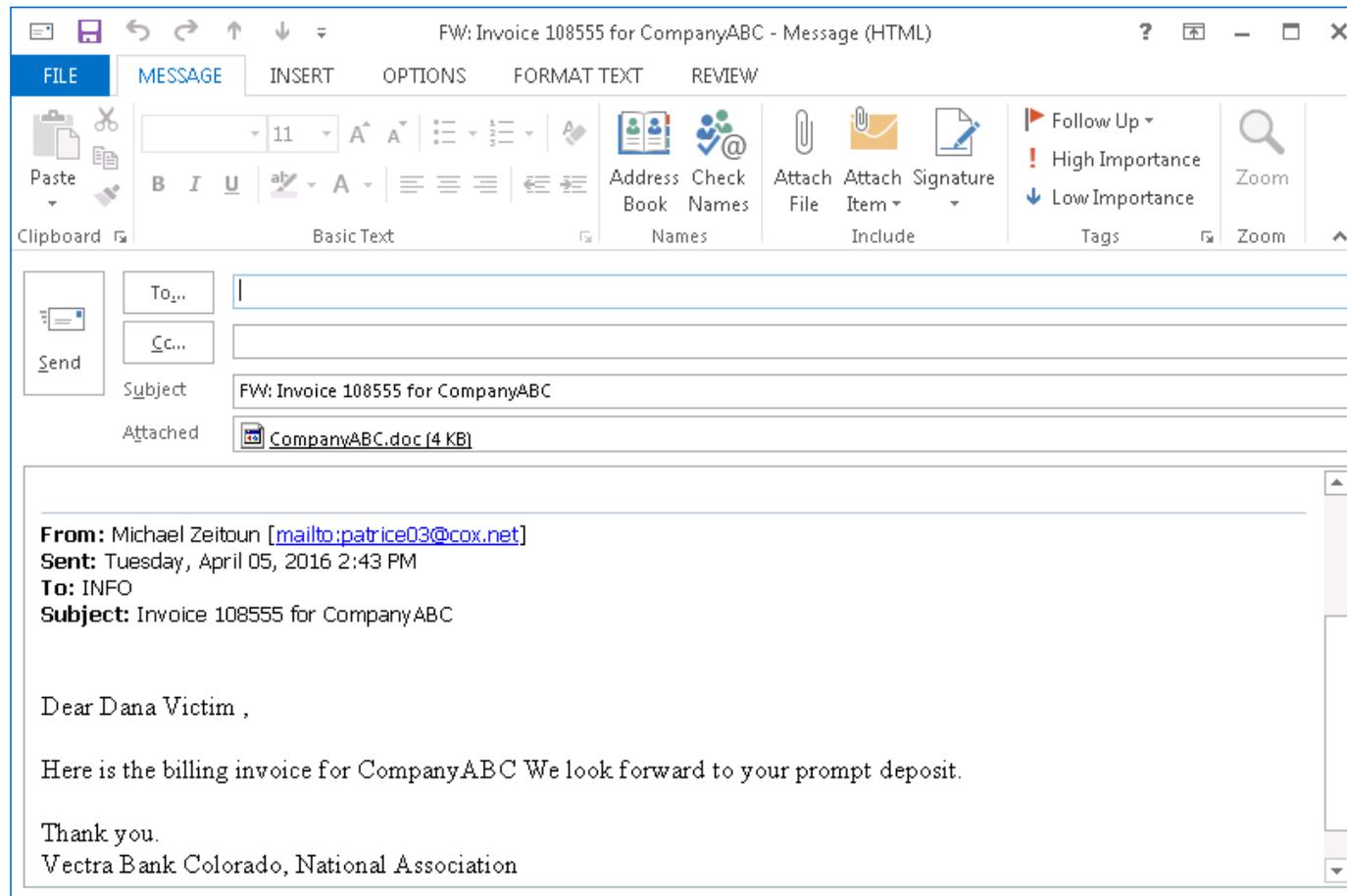
Social media and phishing

Social engineering at its finest

- Participation in social media can make an individual an easy target.
- Makes it easy to do recon on targets
- With higher volume, comes “lazy clicks.”
- Attackers capitalize on this using “Phishing Campaigns.”
- Phishing provides attackers with two main attack vectors:
 - “Watering Hole” attacks for hijacking credentials
 - Embedded malware for exfiltration user credentials and data, including PII
- Freely available tools allow phishing campaigns to be setup and executed in hours.

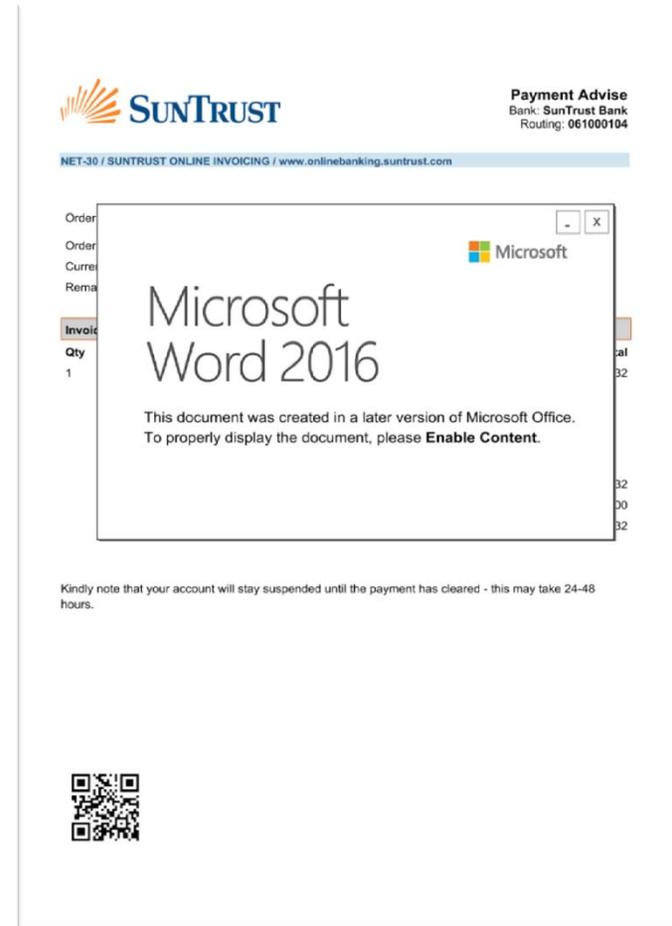
Attack scenario #1

- Phishing emails no longer **look** like a third grader created them.



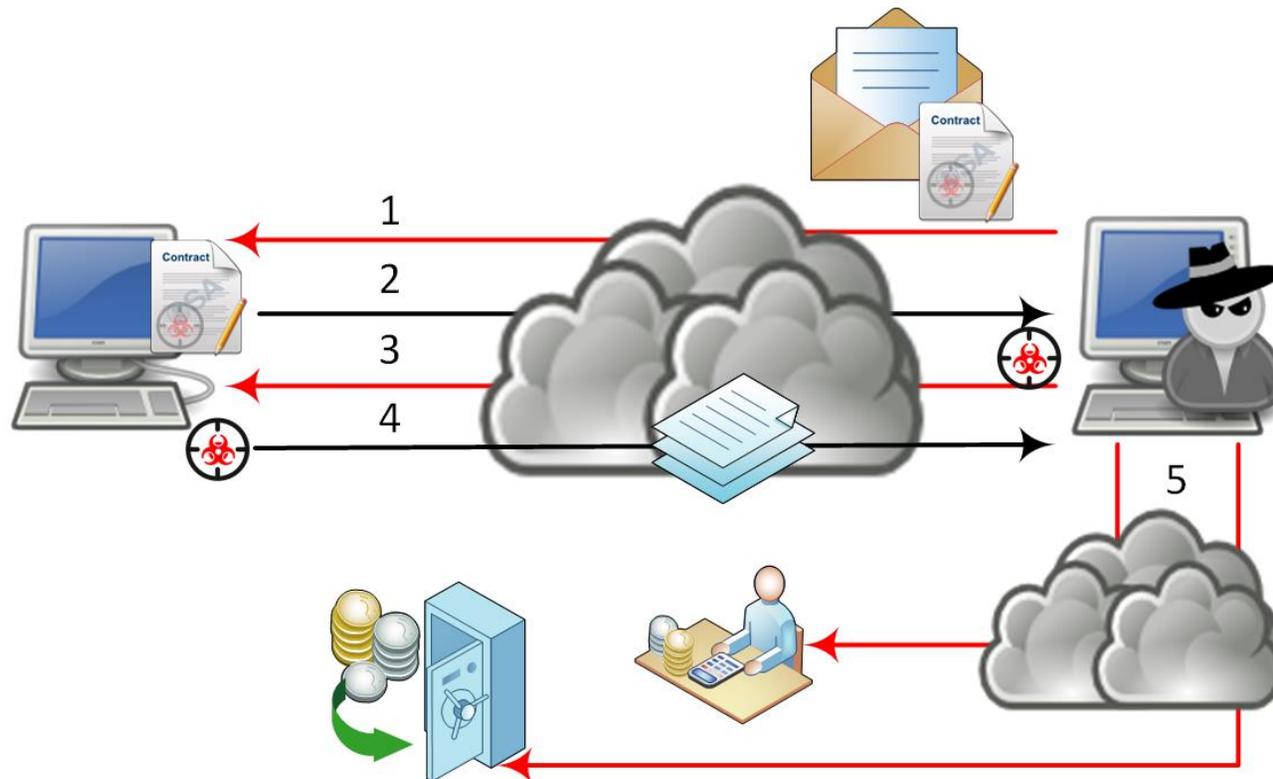
Attack scenario #1 (cont.)

- Phishing emails payloads no longer **look and function** like a third grader created them.
 - Branded invoice
 - Bypasses most anti-virus
 - Embedded macro
 - Macro reaches out to the attacker's servers to download malicious payload
 - Credential Harvester/key logger
 - Ransomware



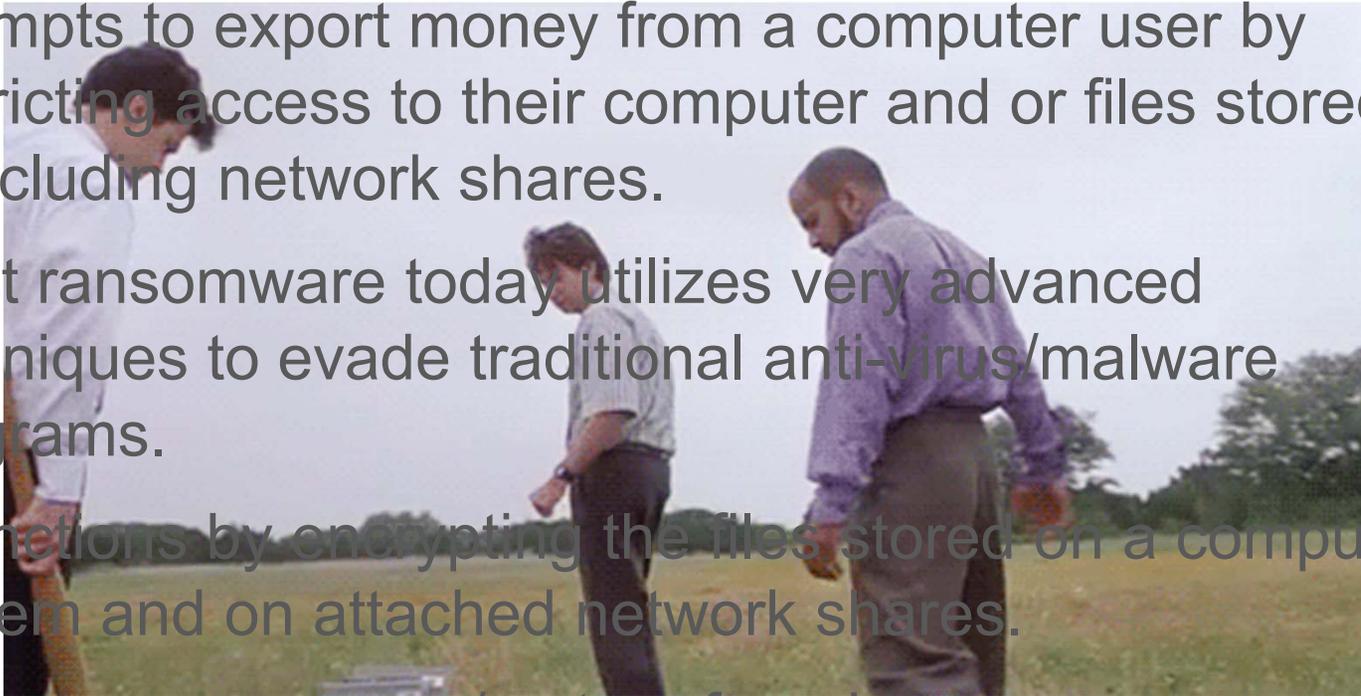
Attack scenario #1 (cont.)

- Phishing emails no longer function like a third grader created them.



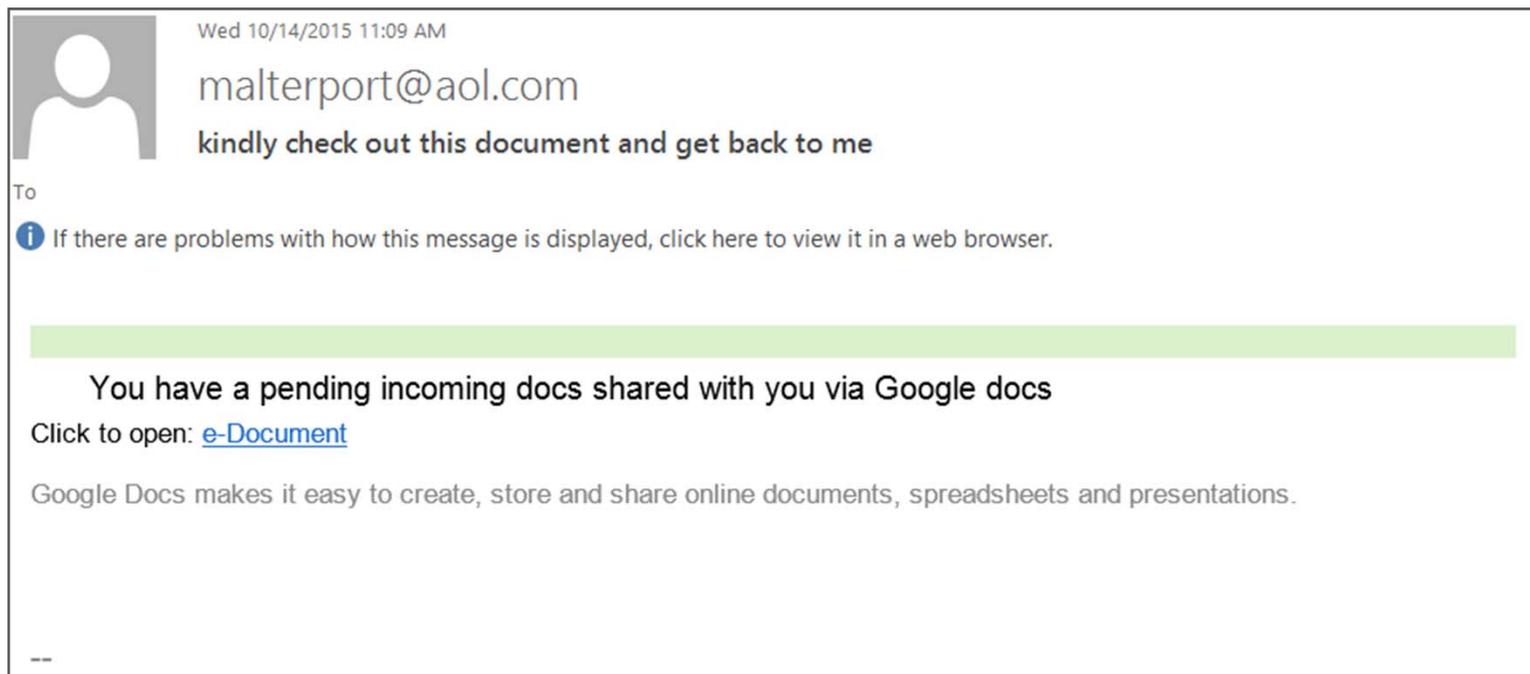
Ransomware

- Ransomware is a form of denial-of-service malware that attempts to export money from a computer user by restricting access to their computer and or files stored on it, including network shares.
- Most ransomware today utilizes very advanced techniques to evade traditional anti-virus/malware programs.
- It functions by encrypting the files stored on a computer system and on attached network shares.
- Options: pay ransom/restore from backups or...



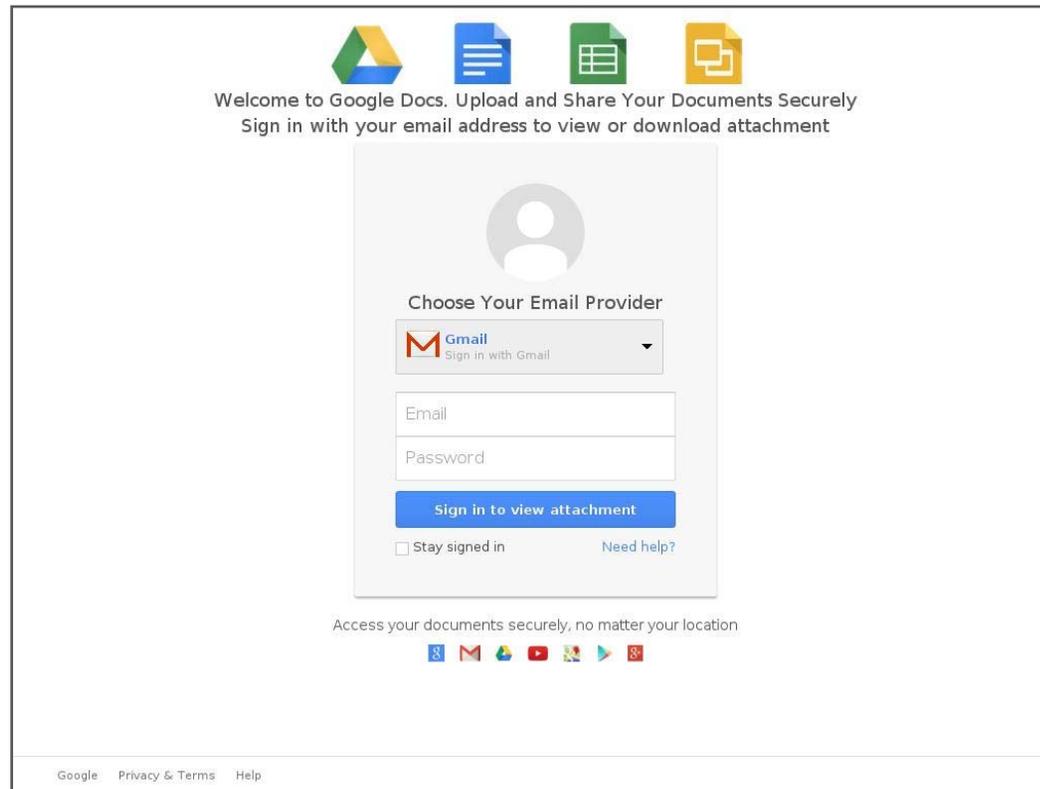
Attack scenario #2

- What is real and what isn't?



Attack scenario #2 (cont.)

- What is real and what isn't?



Attack scenario #3

Hi John,
We are acquiring a foreign company and you are the only one who can help me. No information can be leaked to anyone, even your superiors, or the SEC will cancel the process. Can you assist me with a wire transfer?
-Jim, CEO



Attached is the bank information. The wire transfer for \$750,000 must be completed today or the deal will fall through. Please let me know when this is done.



Sure Jim,
Send me the bank information and I will be happy to take care of this. I understand and respect the confidentiality of this matter. I won't tell anyone.

Attack scenario #3 (cont.)

Well received, thank you. Tomorrow I will be sending you further instructions. Again, please respect the confidentiality of this deal.



Good morning,
An additional wire transfer of \$400,000 must be completed today. I have attached the bank information. Please let me know when this is done. Thank you.



The wire transfer has been sent successfully. Attached is the confirmation. Let me know if you need anything else.

The second wire transfer has been sent. Attached is the confirmation.

Attack scenario #3 (cont.)

Hi John,
This is a scam. DO NOT open any attachments, and DO NOT forward any money. Please inform others about this scam as well.
-Manager

Dear Manager,
I am forwarding this message to you. Do you know what these instructions are? I am concerned about them.
-John

Unfortunately, I already forwarded \$750,000 a few days ago, but was able to cancel another \$400,000 transfer. I trusted the email instructions I received. I'm very sorry for this mistake.

WHAT CAN BE DONE

It's Not Hopeless



What are the risks?

- Best case
 - Preventative controls are in place to identify detect, prevent and block attack.
- Worst case
 - Interruption of business
 - Loss of reputation
 - Loss of public and client trust
 - Endanger financial stability
 - Loss of client PII data may affect vulnerable groups

What should organizations do?

- Comprehensive “security awareness” campaigns
- Security Information and Event Management (SIEM)
- Incident Response Program (CIRT).
- Disaster Recovery Plan (BACKUPS).
- Malware detection/avoidance:
 - End-point protection for hosts
 - Intrusion detection for networks
- Secure coding practices in SDLC
- Formal processes to authorize access to client and employee PII and/or financial information



QUESTIONS AND ANSWERS?



RSM US LLP

80 City Square
Boston

+1 617 912 9000

+1 800 274 3978

www.rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM® and the RSM logo are registered trademarks of RSM International Association. *The power of being understood®* is a registered trademark of RSM US LLP.

© 2016 RSM US LLP. All Rights Reserved.

