

CYBERCRIME

Marshall Area
Chamber of Commerce



October 10, 2017

©2017 RSM US LLP. All Rights Reserved.



About the Presenter

Jeffrey Kline

- 27 years of information technology and information security experience
- Master of Science in Information Systems from Dakota State University
- Technology and Management Consulting with RSM
- Located in Sioux Falls, South Dakota
 - *Rapid Assessment*[®]
 - Data Storage SME
 - Virtual Desktop Infrastructure
 - Microsoft Windows Networking
 - Virtualization Platforms

©2017 RSM US LLP. All Rights Reserved.



Content - Outline

- History and introduction to cybercrimes
- Common types and examples of cybercrime
- Social Engineering
- Anatomy of the attack
- What can you do to protect yourself
- Closing thoughts

©2017 RSM US LLP. All Rights Reserved.



INTRODUCTION TO CYBERCRIME

©2017 RSM US LLP. All Rights Reserved.



Cybercrime

Cybercrime is any type of criminal activity that involves the use of a computer or other cyber device.

- Computers used as the tool
- Computers used as the target



©2017 RSM US LLP. All Rights Reserved.



Long History of Cybercrime

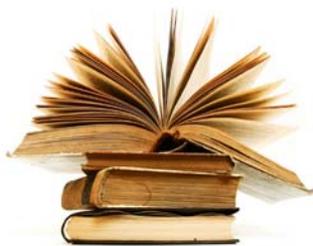
1971	John Draper uses toy whistle from Cap'n Crunch cereal box to make free phone calls
1973	Teller at New York Dime Savings Bank uses computer to funnel \$1.5 million into his personal bank account
1981	First convicted felon of a cybercrime – “Captain Zap” who broke into AT&T computers
1983	UCLA student used a PC to break into the Defense Department’s international communication system
1984	Counterfeit Access Device and Computer Fraud and Abuse Act was passed



©2017 RSM US LLP. All Rights Reserved.



Long History of Cybercrime (continued)



1994	Russian hackers steal \$10 million from Citibank and distribute the money to bank accounts around the world
1995	European Trekkies / hackers compromised Newscorp / SKY-TV to allow illegal access to Star Trek re-runs in Germany
1999	The Melissa worm was one of the first to automatically propagate via email
2002	British hacker accessed 97 US Air Force, Army, Navy, NASA, Pentagon, and DoD computers – looking for evidence of UFOs.
2016	Hacked American election?

©2017 RSM US LLP. All Rights Reserved.



2017's Latest Trends in Cybercrime

- Politically-motivated attacks are on the rise
- Increased attention to public utilities being paid by foreign hackers
- Distributed denial of service (DDOS) attacks using the Internet of things (IoT)
- Increasing sophistication in spear phishing attacks
- Cyber criminals are using tools and techniques to make detection even more difficult
- Zero-day attacks are on the decline

©2017 RSM US LLP. All Rights Reserved.



Cybercrime Facts

- Cybercrime has recently surpassed illegal drug trafficking as a criminal money-maker
- A personal identity is stolen once every 3.1 seconds as a result of cybercrime
- Nearly half of all cybercrimes are committed against small businesses
- Exponential growth in the number of potential victims including: smartphones, cars, railways, planes, power grids, security cameras, refrigerators, garage door openers, etc.
- Some countries, including the UK, see cybercrime surpassing all other traditional crime

©2017 RSM US LLP. All Rights Reserved.



Crime-as-a-Service

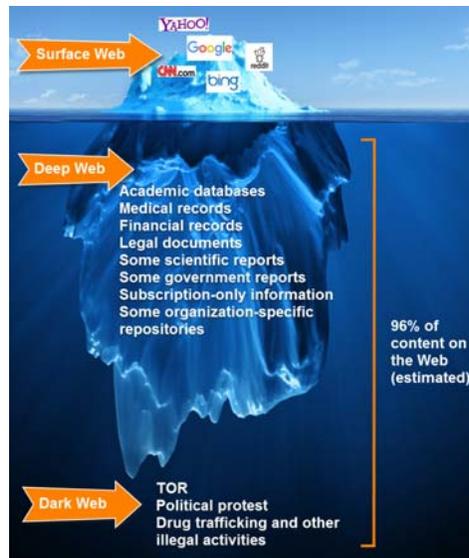
- Growing industry of hackers for hire
- Hacking tools for sale
- Digital currency laundering services
- Hosting services designed for malware
- “Customer service” centers for ransomware
- The Dark Web is home to eBay-like clearing houses for a huge array of criminal services and products



©2017 RSM US LLP. All Rights Reserved.



Crime-as-a-Service – Dark Web



©2017 RSM US LLP. All Rights Reserved.

Digital Currencies

- Bitcoin is the most commonly used digital currency
- Relies on a decentralized ledger called a blockchain
- New Bitcoins are created through minting
- Pseudonymous
- Bitcoin exchanges buy/sell Bitcoins
- Price fluctuates with exchange rate



Today's Exchange Rate: 1 Bitcoin =
\$4,638

©2017 RSM US LLP. All Rights Reserved.



Cybercrime is increasing

2016 saw a **40%** increase in data breaches over 2015, and 2017 is expected to have a **larger increase** yet



©2017 RSM US LLP. All Rights Reserved.



High cost of lost data

Data breaches cost on average **\$158** per lost record



©2017 RSM US LLP. All Rights Reserved.



Huge global costs



Global cost of cybercrime is estimated to hit

\$2 trillion

by 2019

©2017 RSM US LLP. All Rights Reserved.



Data loss happens fast...

68%



of data breaches result in the loss of data within the first



24

hours

©2017 RSM US LLP. All Rights Reserved.



...but our response is slow

< 2%



of data breaches are discovered within



24

hours of occurring



©2017 RSM US LLP. All Rights Reserved.

Persistent threats

Attackers are in a network an average of

200

days before being detected



©2017 RSM US LLP. All Rights Reserved.

Reputation risk

Only
19%
of breaches are self-detected by the
compromised organization



©2017 RSM US LLP. All Rights Reserved.



COMMON TYPES OF
CYBERCRIME

©2017 RSM US LLP. All Rights Reserved.



Business Email Compromise

- Targeted attack on a business
- Based on a compromise of legitimate business email account
- Relies on social engineering and/or data breach
- Mostly fraudulent wire transfers, but sometimes other forms of payment (checks)
- From January of 2015 to June 2016, there was a 1,300% increase in losses due to BEC
- Average loss is \$130,000

©2017 RSM US LLP. All Rights Reserved.



BEC – Method 1

- Foreign Supplier
 - Victim is usually a business that has a long history and relationship with a foreign supplier
 - Fraudulent request is made for invoice payment to a different account
 - Email request will very-closely spoof legitimate request and will be difficult to identify as fraudulent
 - Sometimes also conducted by phone call or fax.



©2017 RSM US LLP. All Rights Reserved.



BEC – Method 2

- Business Executive
 - Email account of executive is either spoofed or hacked
 - Wire transfer request is made by the “executive” to another employee
 - Fraudulent request may also be made to the company’s financial institution
 - Request usually has an urgent nature



©2017 RSM US LLP. All Rights Reserved.



BEC – Method 3

- Employee Email
 - A business employee has their email hacked
 - Employee’s email history and contacts are studied
 - Fraudulent requests for payments are made to other businesses with whom the employee has relationships



©2017 RSM US LLP. All Rights Reserved.



BEC – Method 4

- Attorney
 - Fraudsters impersonate lawyers or representatives of law firms
 - Victims are pressured to act quickly and secretly
 - Funds transfers are requested
 - Usually happens late in the day



©2017 RSM US LLP. All Rights Reserved.



BEC – Method 5 (emerging)

- Data Theft
 - Business executive email is used
 - Victim is usually HR or payroll employee
 - Fraudulent request is usually for W-2 information or other personally identifiable information (PII)
 - First began happening in 2016

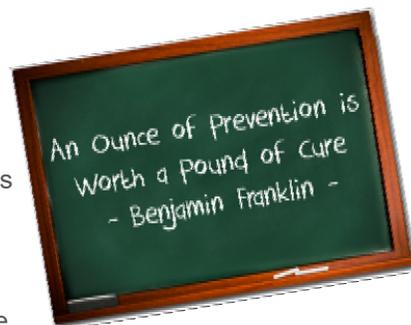


©2017 RSM US LLP. All Rights Reserved.



Preventing Business Email Compromise

- Educate and train employees
- Be wary of any urgent request or pressure to act quickly
- Develop processes for wire transfers that require multiple types of authorization
- Ensure all wire transfers correspond to an active purchase order in your system
- Purchase all domain names that are easily mistaken variants of your main domain name
- Create email rules that flag external email
- Sanitize websites and social media of sensitive information
- Do not allow the same employee to initiate and approve wire transfers
- If you are a victim, contact your financial institution and law enforcement immediately.



©2017 RSM US LLP. All Rights Reserved.



Ransomware

- Usually not targeted
- Victim data is encrypted and a ransom is demanded to decrypt data
- Ransom is paid via Bitcoin, wire transfers, and MoneyPak – all difficult or impossible to trace
- Numerous variants with more appearing regularly
- 167 times as much ransomware in 2016 compared to 2015
- Paying the ransom **usually** results in the decrypting of data

©2017 RSM US LLP. All Rights Reserved.



Ransomware (continued)

- Ransoms typically range from 1 or 2 bitcoins to 100 or more bitcoins
- FBI estimates \$24 million was paid in 2015 (U.S.)
- For 2016, that number increased to nearly \$1 billion
- Paying victims have included:
 - City and county governments
 - Police and Sherriff departments
 - School districts
 - Hospitals
 - International state governments
 - Businesses and organizations of all sizes
 - Home users
- Studies show that 64% of victims pay the ransom



©2017 RSM US LLP. All Rights Reserved.



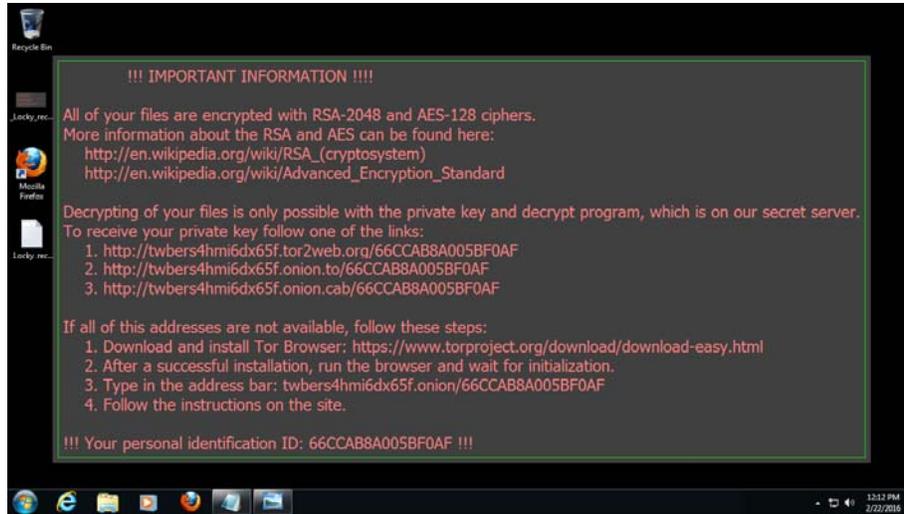
Ransomware (continued)

- Average ransom per machine was \$294 in 2015
- Average ransom per machine was \$679 in 2016
- Over 400 variants in the wild at the end of 2016
- Currently the payload of choice for malicious email campaigns
- Ransomware toolkits are available on the Dark Web
- Relative anonymous nature of digital currency helps protect criminal activity

©2017 RSM US LLP. All Rights Reserved.



Ransomware Example – Locky (2016’s biggest)



©2017 RSM US LLP. All Rights Reserved.

RSM

Ransomware Example - PRISM



©2017 RSM US LLP. All Rights Reserved.

RSM

Ransomware Example



©2017 RSM US LLP. All Rights Reserved.



Ransomware Example - TeslaCrypt



©2017 RSM US LLP. All Rights Reserved.



Ransomware Example - Demonslay



©2017 RSM US LLP. All Rights Reserved.



Ransomware Example – Demonslay (continued)



©2017 RSM US LLP. All Rights Reserved.



Ransomware Example – CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR / similar amount** in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/15/2013 8:44 PM

Time left
57 : 45 : 37

Next >>

©2017 RSM US LLP. All Rights Reserved.



Ransomware Example – CryptoWall

Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **10/06/14 - 08:14** the cost of decrypting files will increase 2 times and will be **1000 USD/EUR**

Prior to increasing the amount left:
119h 58m 24s

Your system: Windows 7 (64) First connect IP: [redacted] Total encrypted 28 files.

Refresh Payment FAQ Decrypt 1 file for FREE Support

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?

bitcoin

- You should register Bitcoin wallet** ([click here for more information with pictures](#))
- Purchasing Bitcoins** - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:
 - Coin.mx** - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire
 - LocalBitcoins.com** - Service allows you to search for people in your community willing to sell bitcoins to you directly.
 - coinm.com** - Another fast way to buy bitcoins
 - bt2mark.co** - Buy Bitcoins Instantly for Cash
 - How To Buy Bitcoins** - An international directory of bitcoin exchanges.
 - Cash Into Coins** - Bitcoin for cash.
 - CoinJar** - CoinJar allows direct bitcoin purchases on their site.
 - inopex.com**
 - buybitcoins.com**
 - ZipZap** - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
- Send 0.79 BTC to Bitcoin address:** 1175Lmazbby614zs05Lw46x1mJv0eV [Get QR code](#)
- Enter the Transaction ID and select amount:**
[input field] 0.79 BTC == 500 USD

Note: Transaction ID - you can find in detailed info about transaction you made (example 442144fc56e03938660929c40f54f19a27c42675d3e23a08114c4c12)

©2017 RSM US LLP. All Rights Reserved.



Ransomware Example – CryptoWall variant

Is the content of the files that you have watched not readable?
It is normal because the files' names, as well as the data in your files have been encrypted.

Congratulations!!!
You have become a part of large community CryptoWall.

.....

If you are reading this text that means that the software CryptoWall has removed from your computer.

.....

What is encryption?
Encryption is a reversible transformation of information in order to conceal it from unauthorized persons but providing at the same time access to it for authorized users. become an authorized user and make the process truly reversible i.e. to be able to decrypt your files you need to have a special private key. In addition to the private key you need the decryption software with which you can decrypt your files and return everything in its place.

.....

I almost understood but what do I have to do?
The first thing you should do is to read the instructions to the end.

Your files have been encrypted with the CryptoWall software, the instructions that you find in folders with encrypted files are not viruses, they are your helpers. After reading this text 100% of people turn to a search engine with the word CryptoWall where you'll find a lot of thoughts, advice and instructions. Think logically - we are the ones who closed the lock on your files and we are the only ones who have this mysterious key to open them. Any of your attempts to restore your files with the third-party tools can be fatal for encrypted files. The fact is that changing data within the encrypted file (as 100% of software to restore files do this, except the special decryption software) you break damage to the file and will be impossible to decrypt the file. It is the same as to collect a mosaic when some mosaic items were lost, broken or not put in its place - the picture will not emerge, the software to restore the files will be able to lay down the picture, and ruin it completely and irreversibly. Using the software to restore files can ruin your files forever, only through your fault. Remember that any intervention of the extraneous software to restore files encrypted with the CryptoWall software may be the point of no return.

.....

In case if these simple rules are violated we will not be able to help you, and we will not try because you have been warned. For your attention the software to decrypt the files (as well as the private key that come fitted with it) is a paid product.

After purchasing the software package you can:

©2017 RSM US LLP. All Rights Reserved.



Prepare for Ransomware

- It is not a matter of **IF**, but a matter of **WHEN**
- Excellent user training can help avoid problems
- Refine and restrict permissions to network files
- Frequent backups stored off-line
- Detection tools
- Test backup capabilities
- Get a Bitcoin wallet – just in case!



©2017 RSM US LLP. All Rights Reserved.



Malvertising

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse auctor nunc ac molestie vestibulum. Sed quis mauris sit amet odio finibus porta sed gravida nisi. Nulla consequat sollicitudin ante sed tincidunt. Maecenas in malesuada leo. Integer vitae egestas ex, ac bibendum lacus. Pellentesque luctus, neque vel fringilla euismod, dolor sapien hendrerit purus, a eleifend quam ex at enim. Maecenas in sagittis justo. Nunc gravida turpis nec rutrum sodales. Nam in auctor erat, quis pulvinar purus. Etiam turpis risus, egestas a egestas vitae, cursus in mauris. Mauris condimentum orci in nisi placerat, mattis dictum dui tristique.

Quisque gravida imperdiet imperdiet. Praesent semper odio auctor eros ornare eleifend. Sed vitae congue justo. Donec placerat sed orci hendrerit vehicula. Nunc vel molestie nisi. Vestibulum dignissim rutrum metus sed maximus. Integer elementum leo arcu, quis tristique leo bibendum eget. Duis ut enim a eros blandit efficitur. Donec vitae arcu ac nibh rhoncus varius quis eget tortor. Integer eget vulputate leo. Curabitur vitae augue sem. Phasellus vitae aliquet urna, quis tempor leo. Donec auctor in ante sit amet mattis. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae;

Nam dignissim elit eu neque dapibus, nec semper quam fringilla. Donec vel purus a lorem volutpat gravida at eu sapien. Praesent interdum scelerisque enim id elementum. Proin euismod tempus urna, quis condimentum nulla. Integer interdum iaculis lacinia. Maecenas id nibh ac magna imperdiet lacinia. Sed porta libero sit amet pellentesque bibendum. Proin in viverra nibh, nec pharetra odio. Maecenas bibendum nisi est, ut placerat nisi finibus sit amet. Pellentesque interdum dictum tortor non interdum.

Bored employee finds clubbing baby seals on the Internet. What he does next will blow your mind...

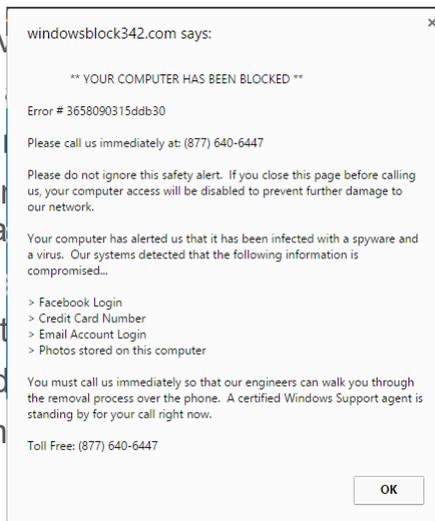


©2017 RSM US LLP. All Rights Reserved.



Malvertising (continued)

- Online ads and v
- Often displayed
- Very easy for cu
- Some malvertisi
- relies on vulnera
- 4 to 5x increase
- Difficult to detect
- At times, exceed
- “Kovter” is the m



Content on k – it



He Found A Hidden Room In This Old Attic, But He...

Your Tailored News



Obama Quietly Gives 119 Million Americans \$42.4b i...

Oxford Communique Subscription

©2017 RSM US LLP. All Rights Reserved.



Malvertising (continued)

The screenshot shows a web browser displaying a Microsoft support page. A prominent blue banner at the top of the page content area contains the text "Call for support: +1 (877) 640-6447" repeated twice. Below the banner, there are navigation links: "Manage my account", "Ask the community", "Contact Answer Desk", and "Find downloads". A section titled "I need help with..." features three icons: Windows, Windows Phone 8, and Lumia devices. The RSM logo is visible in the bottom right corner of the page. The browser's address bar shows a URL from windowsblock342.com.

SOCIAL ENGINEERING

The slide features a large blue rectangular area with the text "SOCIAL ENGINEERING" in white, bold, uppercase letters. To the left of this area is a vertical green bar, and to the far left is a thin grey bar. The RSM logo is located in the bottom right corner of the slide. A small copyright notice "©2017 RSM US LLP. All Rights Reserved." is visible in the bottom left corner.

Social Engineering Definitions

Any act that influences a person to take an action that may or may not be in their best interest.

An attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.

The art and science of getting people to comply with your wishes.

Using non-technical or low-technology means – such as lies, impersonation, tricks, bribes, blackmail, and threats – to attack information systems.

Hacking using brains instead of computer brawn.

©2017 RSM US LLP. All Rights Reserved.



Social Engineering

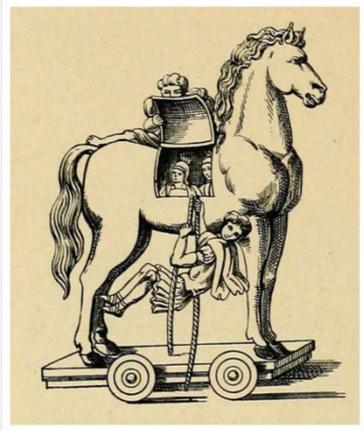
- Used to initiate or perpetuate a cybercrime
- Why do the hard work when someone else will do it for you?
- Relies on human psychology
- Human's curiosity, greed, or willingness to help is used against them
- Most successfully-used vulnerability
- Most frequently-used exploit



©2017 RSM US LLP. All Rights Reserved.



Classic Example – Greeks and the Trojan Horse



- Source of the current security term, “Trojan horse”
- Relied on the Trojan’s human nature to bring the war trophy inside their gates
- That night, the hidden soldiers exited the horse and opened the gates of Troy, letting in the Greek soldiers

©2017 RSM US LLP. All Rights Reserved.



Classic Example - William Thompson

- Caused the term “confidence man” (con man) to be coined
- Operated in New York City in the late 1840s
- Simply asked people on the street if they would have confidence in him to hold their watch or money until tomorrow
 - People assumed he was an old acquaintance



©2017 RSM US LLP. All Rights Reserved.



Classic Example – Joseph “Yellow Kid” Weil

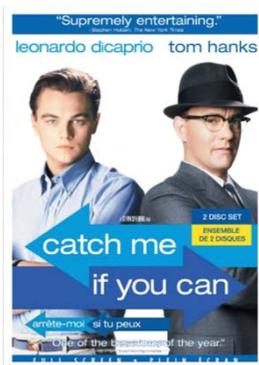


- Started out in the 1890s selling an Elixir that was mainly just rainwater
- Said, “A chap who wants something for nothing usually winds up with nothing for something”
- Often targeted bankers
- Sold fake claims to oil-rich land
- Swindled Benito Mussolini out of \$2 million by selling land he didn’t own
- Sold talking dogs
- Stole over \$8 million in his lifetime

©2017 RSM US LLP. All Rights Reserved.



Classic Example – Frank Abagnale



- Used Social Engineering to:
 - Defraud his father
 - Commit bank fraud
 - Impersonate professions:
 - Airline pilot
 - Teaching assistant
 - Doctor
 - Attorney
- Life story inspired the film, *Catch Me If You Can*, a Broadway musical, and an autobiography



©2017 RSM US LLP. All Rights Reserved.



Recent Example – Alcona County, Michigan

- Alcona County, Michigan treasurer embezzled \$1.25 million of the county's \$4 million operating budget in 2007
- Used the money to pay a 419 scammer
 - Nigerian prince
 - Spanish prisoner
- The treasurer believed the emails from the scammer
- Received 14 years in prison



©2017 RSM US LLP. All Rights Reserved.



Recent Example - Target

- One of the largest attacks of 2013
- Hackers stole 40 million credit card numbers from POS systems
- Attackers gained access by using a phishing email sent to Target's HVAC subcontractor
- Illustrated that the weakest link can be a third-party contractor, supplier, or partner



©2017 RSM US LLP. All Rights Reserved.



Real World Examples

- Small Town



©2017 RSM US LLP. All Rights Reserved.



Personal Example

Mon 03/06/2017 9:36 AM
 Delta Air Lines <DeltaAirLines@t.delta.com>
 Your Flight Ticket Invoice 51634 - jeffrey.kline
 To: Kline, Jeffrey

This is a payment confirmation e-mail for the ticket you ordered on Delta.com website.

Your credit card has been charged.

Flight Number : WA618348
 Date : MAR 7 2017, 17:45 CDT
 Departure : Washington, DC

You can download and print your ticket from our website :
https://www.delta.com/tickets/viewOrder.do?order_id=70126_742&flight=WA618348

For more information regarding your order, contact our technical support by visiting :
https://www.delta.com/content/www/en_US/support.html
 Thank you for flying with Delta Airlines

©2017 Delta Air Lines, Inc.

This is a payment confirmation e-mail for the ticket you ordered on Delta.com website.

Your credit card has been charged.

Flight Number : WA618348
 Date : MAR 7 2017, 17:45 CDT
 Departure : Washington, DC

<http://www.malton.com.my/api/getn.php?id=amvmznjles5rbgluzubty2dsywryzckuy29t>

You can download and print your ticket [Click to follow link](#)
https://www.delta.com/tickets/viewOrder.do?order_id=70126_742&flight=WA618348

MALTON.COM

The owner of **malton.com** is offering it for sale for an asking price of 12000 Euro

BUY THIS DOMAIN
 The owner of **malton.com** is offering it for sale for an asking price of 12000 Euro
 More details [.sedo](#)

Related Links

- Malton Hotel
- Killarney
- Malton
- Malton
- Hotel Software
- Leeds Hotel
- Hotel York UK
- Hotel in Bradford
- Hull Hotel
- A Forex

.sedo This domain was generated by the domain owner using form 2006030200. *Disclaimer: Sedo members do not warrant any third party information. Malton.com is only available in some cases. It is not intended to sell any domain or to provide any information or representation.

©2017 RSM US LLP. All Rights Reserved.



Social Engineering may have changed the world

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* john.podesta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> john.podesta@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

©2017 RSM US LLP. All Rights Reserved.

```
*From:* Charles Delavan <cdelavan@hillaryclinton.com>
*Date:* March 19, 2016 at 9:54:05 AM EDT
*To:* Sara Latham <slatham@hillaryclinton.com>, Shane Hable <shable@hillaryclinton.com>
*Subject:* *Re: Someone has your password*

Sara,

This is a legitimate email. John needs to change his password immediately,
and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security to do both.
It is absolutely imperative that this is done ASAP.
```



Types of Social Engineering

- Pretexting
- Diversion
- Phishing
- Vishing / Phone Phishing
- Spear Phishing
- Water Holing
- Baiting
- Quid Pro Quo
- Tailgating



©2017 RSM US LLP. All Rights Reserved.



Types of Social Engineering - Pretexting

- Social engineer creates a fabricated scenario
- May pose as a representative of a legitimate business that needs sensitive information
- False sense of trust created
- Can involve physical element – showing up and pretending to be someone they are not



©2017 RSM US LLP. All Rights Reserved.



Types of Social Engineering - Diversion

- Social engineer tricks the victim into delivering goods or data to an unsafe location
- Common con in the physical world where delivery drivers are told to change the delivery to a place “around the corner”
- Persuades victim to send data to a location that results in theft of data



©2017 RSM US LLP. All Rights Reserved.



Types of Social Engineering - Phishing

- Most common form of social engineering
- Social engineer sends an email to a huge list of potential victims
 - Estimated that 200 million are sent each day
 - 15 million of which make it through spam filters
 - Around 1/3 of those are opened
 - 12% of those opening messages click on the links
 - 10% of those who clicked share their information (about 80,000 people per day)
- Email attempts to look like legitimate correspondence from a bank, credit card company, PayPal, Ebay, etc.
- Malicious code in the email
- Directs victim to a fake site where credentials are stolen
- Downloads and installs malware / ransomware



©2017 RSM US LLP. All Rights Reserved.



Types of Social Engineering – Vishing (Phone Phishing)

- Phishing using a telephone
 - Real human caller
 - War dialer
- Victims receive phone calls from social engineers attempting to steal personal data or money
- May use caller ID spoofing
- Inbound vishing uses sophisticated IVR systems
- Close cousin – “smishing” uses the same concept, but with text messaging (SMS)



©2017 RSM US LLP. All Rights Reserved.



Types of Social Engineering – Spear Phishing

- Targeted phishing / vishing
- Social engineer does research to make phishing attempts more successful
 - Company website
 - Blogs
 - Social media
- Spear phishing is often how business email compromise starts
- Goal is the same as with phishing:
 - Steal credentials
 - Install malware for further attacks



©2017 RSM US LLP. All Rights Reserved.



Types of Social Engineering – Water Holing

- Social engineers target an industry, interest group, organization, etc.
- Website commonly used by victims is studied and ultimately compromised
- Malicious code is delivered to users who visit the site
- Code is used to gain access into victims' computers



©2017 RSM US LLP. All Rights Reserved.



Types of Social Engineering – Baiting

- Social engineer lures the victim into opening a malicious file, usually relying on curiosity or greed
- Physical media is often used
- Left in bathrooms, parking lots, break rooms, elevators, etc.
- Online forms of baiting include malvertising, free downloads, etc.
- Payload usually gives attackers access to victims' computers



©2017 RSM US LLP. All Rights Reserved.



Types of Social Engineering – Quid Pro Quo

- Social engineer tricks the victim into doing something in exchange for a service or action
- Similar to baiting
- Often the social engineer poses as a company IT person and asks the victim to perform some action in order to upgrade their system



©2017 RSM US LLP. All Rights Reserved.



Types of Social Engineering – Tailgating

- Typically a physical method of social engineering
- Social engineer gains physical entry to a secure area
- Follows a legitimate employee
- Asks an employee for entry because they forgot their badge
- Poses as a delivery driver with many boxes and asks to have door held



©2017 RSM US LLP. All Rights Reserved.



Stopping Social Engineering

- Train employees
 - Train employees
 - Train employees
 - Test employees
-
- Maintain as good security on all the “technical parts” of the environment as absolutely possible



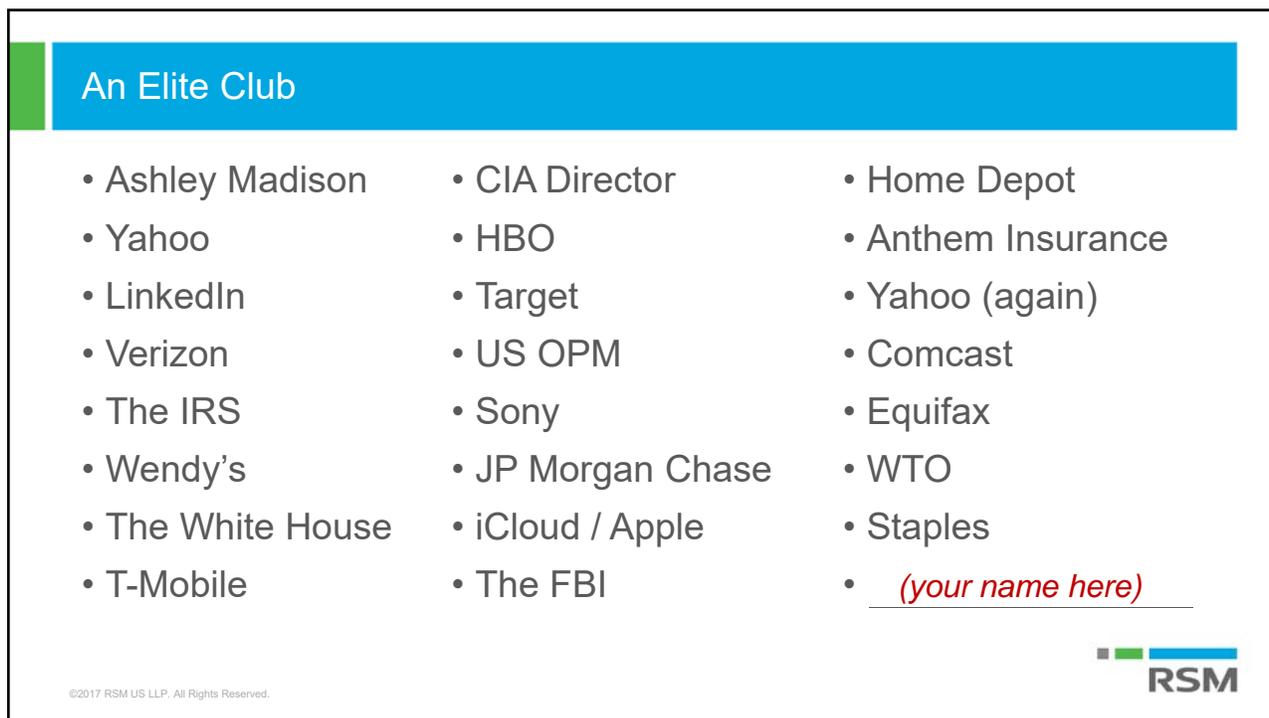
©2017 RSM US LLP. All Rights Reserved.





ANATOMY OF THE ATTACK

©2017 RSM US LLP. All Rights Reserved.

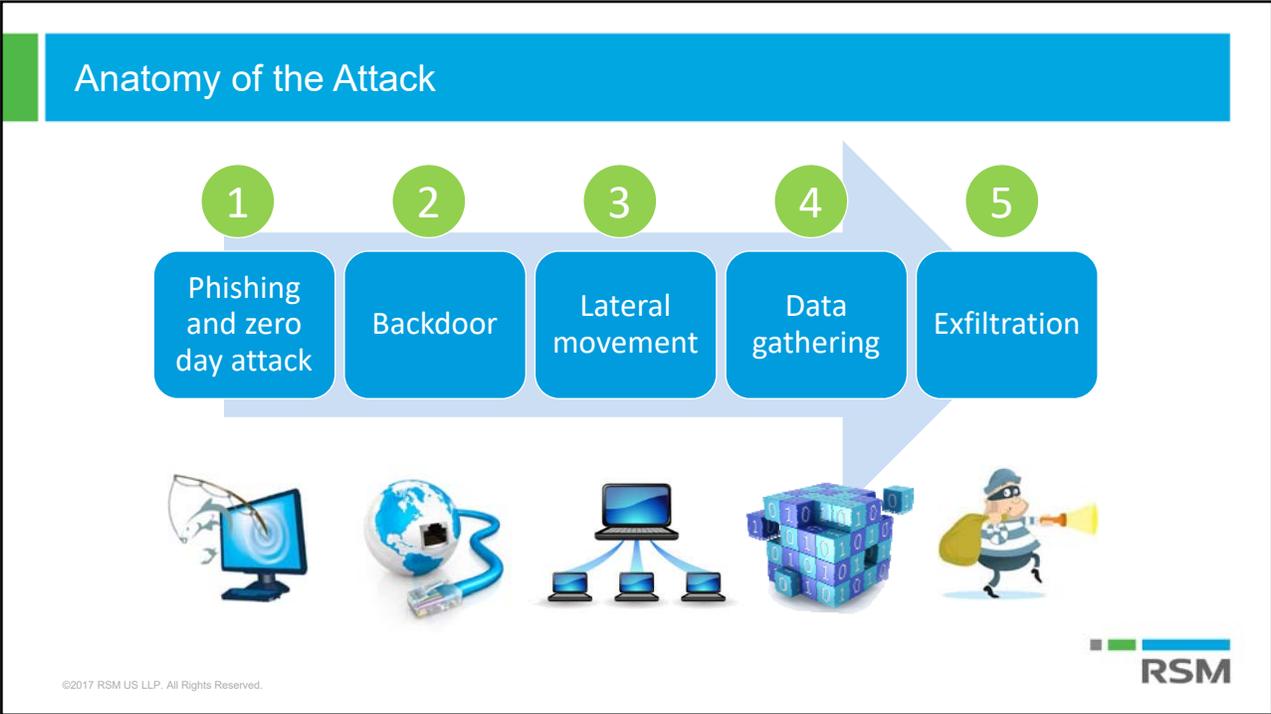


An Elite Club

- Ashley Madison
- Yahoo
- LinkedIn
- Verizon
- The IRS
- Wendy's
- The White House
- T-Mobile
- CIA Director
- HBO
- Target
- US OPM
- Sony
- JP Morgan Chase
- iCloud / Apple
- The FBI
- Home Depot
- Anthem Insurance
- Yahoo (again)
- Comcast
- Equifax
- WTO
- Staples
- *(your name here)*

©2017 RSM US LLP. All Rights Reserved.





WHAT CAN YOU DO?

©2017 RSM US LLP. All Rights Reserved.

Three basic steps to prevent cybercrime



1. Get Real
2. Get Help
3. Get Educated

©2017 RSM US LLP. All Rights Reserved.



1: Get Real



- Understand and appreciate the threats that exist
- Make cybersecurity an organizational priority from the board/CEO/owner down
- Never assume safety from anonymity, size, or geography
- Know that information security is a never-ending project
- Recognize that you may be outnumbered but you don't have to be outsmarted

©2017 RSM US LLP. All Rights Reserved.



2: Get Help



- Unless you are a huge company, you most likely cannot adequately handle all information security functions internally
- Perform security review, audit, assessment, etc., even if not required by regulation
- Enlist a vendor to assist with patch management, anti-virus, etc.
- Order regular penetration tests and social engineering tests

©2017 RSM US LLP. All Rights Reserved.



3: Get Education



- Subscribe to cybersecurity newsletters and feeds
- Keep cybersecurity a top-of-mind subject throughout the organization
- Provide cybersecurity and social engineering training to employees
- Test employees for adherence to cybersecurity standards
- Understand what rights users have to network resources

©2017 RSM US LLP. All Rights Reserved.





CLOSING THOUGHTS

©2017 RSM US LLP. All Rights Reserved.



An ounce of prevention...



99.9%

of vulnerability exploits occur **more than a year** after the vulnerability was disclosed

©2017 RSM US LLP. All Rights Reserved.



...is 10 patches away



97%

of exploits occurred from a list of **just 10** published vulnerabilities

©2017 RSM US LLP. All Rights Reserved.



Humans...

30%

of recipients now **open** phishing messages



©2017 RSM US LLP. All Rights Reserved.



...often the weakest link



12%
of recipients **click on** phishing attachments

©2017 RSM US LLP. All Rights Reserved.



Too many privileges



55%
of insider incidents involve abuse of privileges

©2017 RSM US LLP. All Rights Reserved.



Passwords!



39%
of passwords are only **8 characters** long and can be cracked in **under one day**

©2017 RSM US LLP. All Rights Reserved.



QUESTIONS AND ANSWERS?



©2017 RSM US LLP. All Rights Reserved.





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.

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.

© 2017 RSM US LLP. All Rights Reserved.



©2017 RSM US LLP. All Rights Reserved.