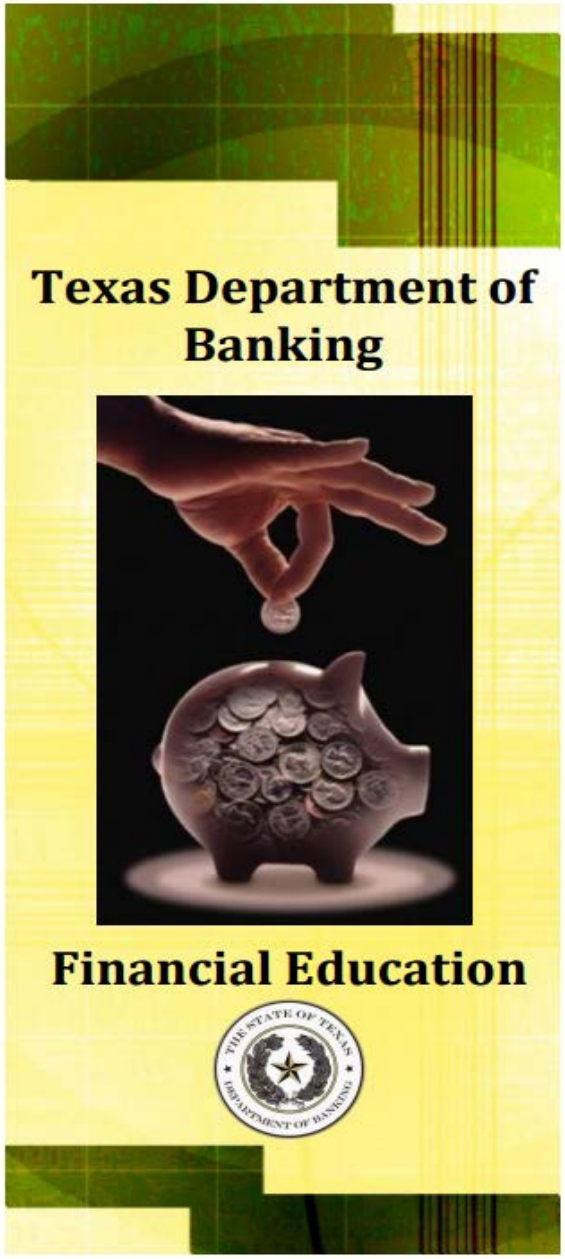


Texas Department of Banking

CYBERSECURITY AWARENESS FOR MONEY SERVICES BUSINESSES

November 3, 2016

Leilani Lim-Villegas
Financial Education Coordinator

Cybersecurity Awareness

Ruth Norris, IT Security Examiner
Texas Department of Banking

Cybersecurity: Awareness and Assessment is Key!

Why do we need to assess cybersecurity?

- Existing vulnerabilities continue to be exploited.
- New platforms create new ways to exploit Financial Institutions and customers.
- Lines between cyber actors are blurring as tool are commercialized.
- Use of social networking enables more effective and targeted attacks
- Malware continues to evolve and now includes data destruction and encryption
- Global unrest results in US symbols, including financial institutions being targeted

According to the Symantec 2015 Internet Security Threat Report…

- A new zero-day vulnerability is discovered each week.
- Half a billion personal records have been stolen or lost.
- Three quarter of websites have vulnerabilities.
- Increase in spear-phishing attacks.
- Ransomware has increased by 35 percent.
- 100 million fake technical support scams blocked.

What are we dealing with?

Source: Symantec 2015 Internet Security Threat Report
https://www.symantec.com/security-center/threat-report

Over Half a Billion Personal Information Records Stolen or Lost in 2015

and more companies than ever not reporting the full extent of their data breaches

36%

of breaches included medical records

The largest number of breaches took place within the Health Services sub-sector, which actually comprised 39 percent of all breaches in the year. This comes as no surprise, given the strict rules within the healthcare industry regarding reporting of data breaches.

39%

120 Incidents

4 Million Identities Exposed

2015 Stats

Total Reported Identities Exposed

numbers in millions

2015	429	+23%
2014	348	-37%
2013	552	

These numbers are likely higher, as many companies are choosing not to reveal the full extent of their data breaches.

Most of an iceberg is submerged underwater, hiding a great ice mass. The number of reported identities exposed in data breaches are just the tip of the iceberg. What remains hidden?

REPORTED IDENTITIES EXPOSED

78 million patient records were exposed at Anthem

22 million personal records were exposed at Office of Personnel Management

2014: 61

2015: 113 +85%

Incidents that did not report identities exposed in 2015

UNREPORTED IDENTITIES EXPOSED

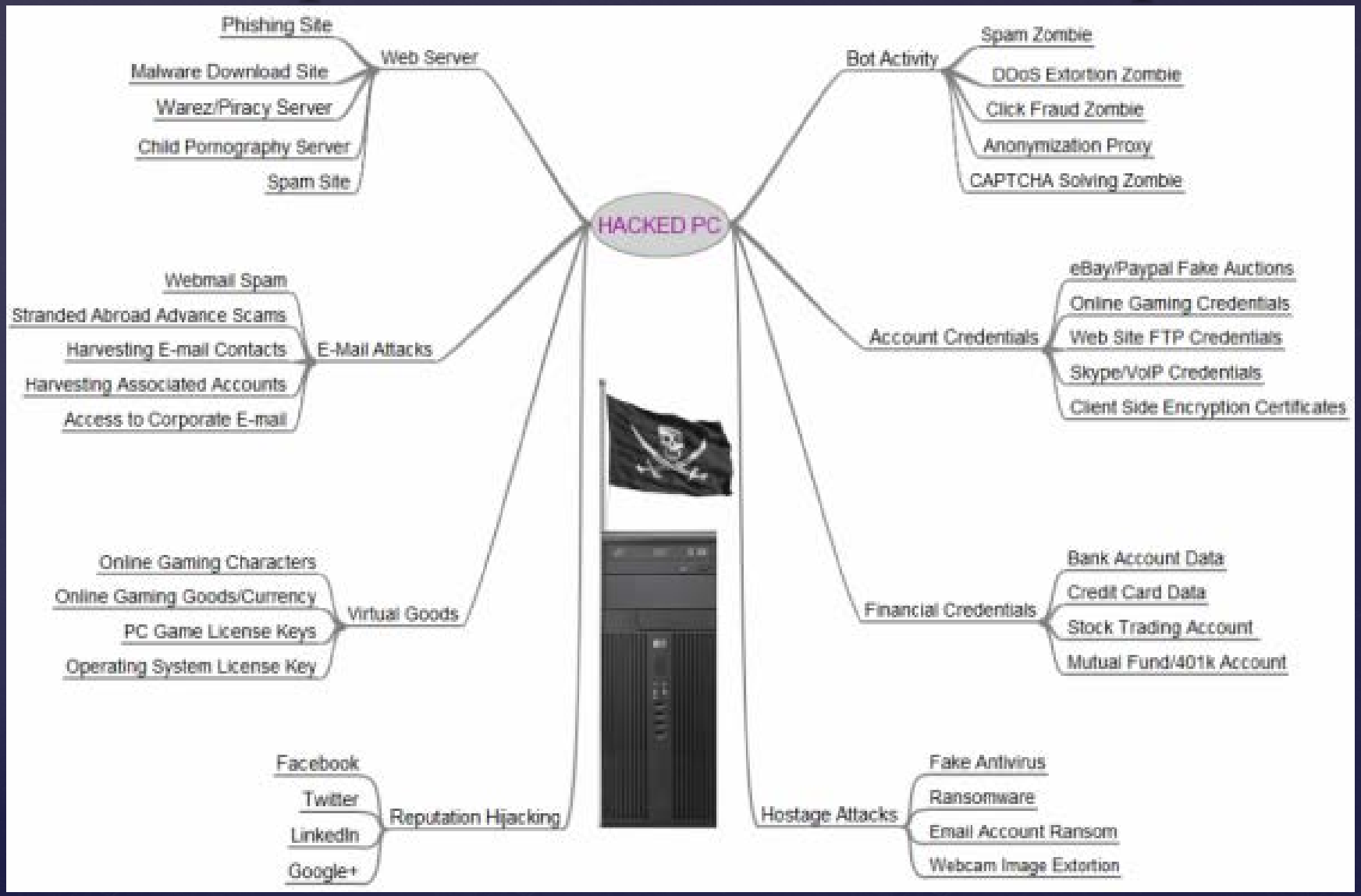
Despite companies' choice not to report the true number of records exposed, hundreds of millions more people may have been compromised.

Given the facts, it is possible that **500** Million* identities were exposed

*estimated

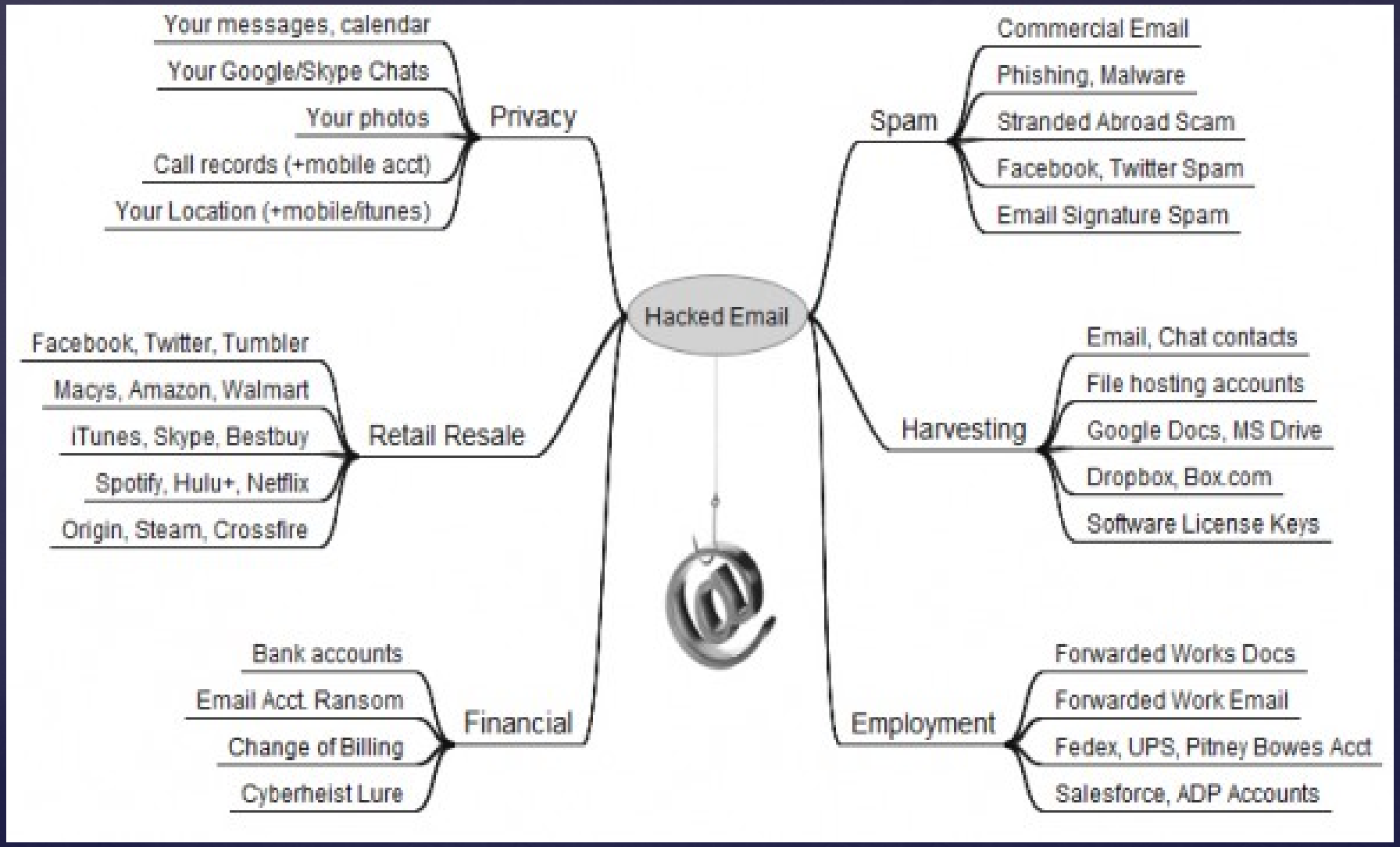
Symantec.

The Impact of A Hacked Computer



What happens when your email is compromised?

Source: Krebs on Security



#ThreatsTrending

- Ransomware
- Business Email Compromise
- Account Takeover
- Destructive Malware
- Human Error
- DDoS Attacks
- Information/Card Breaches

What are we dealing with?

Virus!
https://
Malware

RaNSoMWaRE

AEQUITAS
LIBERTAS
VERITAS
2009
IN CRYPTOGRAPHY WE TRUST

RaNSoMWaRE

What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0.
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1.http: [redacted]
2.http: [redacted]
3.http: [redacted]
4.http: [redacted]

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: paytoc4gtpn5czl2.onion/127gtms
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

Your Personal PAGE: http: [redacted]
Your Personal PAGE(using TOR): [redacted]
Your personal code (if you open the site (or TOR 's) directly [redacted] s

0x000000CE DRIVER_UNLOADED_WITHOUT_CANCELLING_PENDING_OPERATIONS

WINDOWS HEALTH IS CRITICAL
DO NOT RESTART

PLEASE CONTACT MICROSOFT TECHNICIANS

BSOD : Error 333 Registry Failure of operating system - Host :
BLUE SCREEN ERROR 0x000000CE

Please contact microsoft technicians At Toll Free : [redacted]

To Immediately Rectify issue to prevent Data Loss

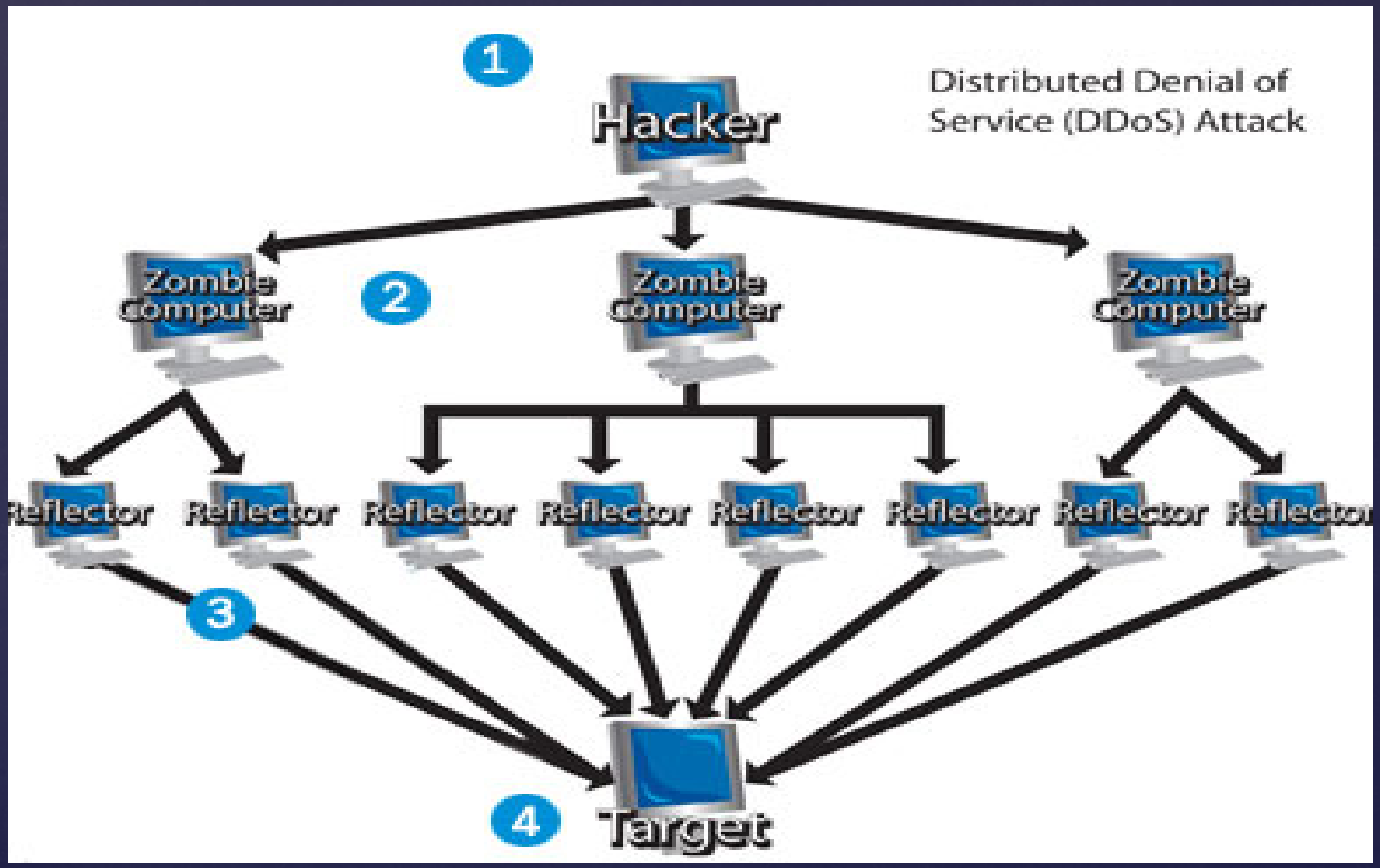
Account Takeover

Account Takeover (**ATO**) is a form of **business ID Theft** in which cyber criminal gains control of a business' bank account by stealing the user IDs and other credentials a business uses for on-line banking.

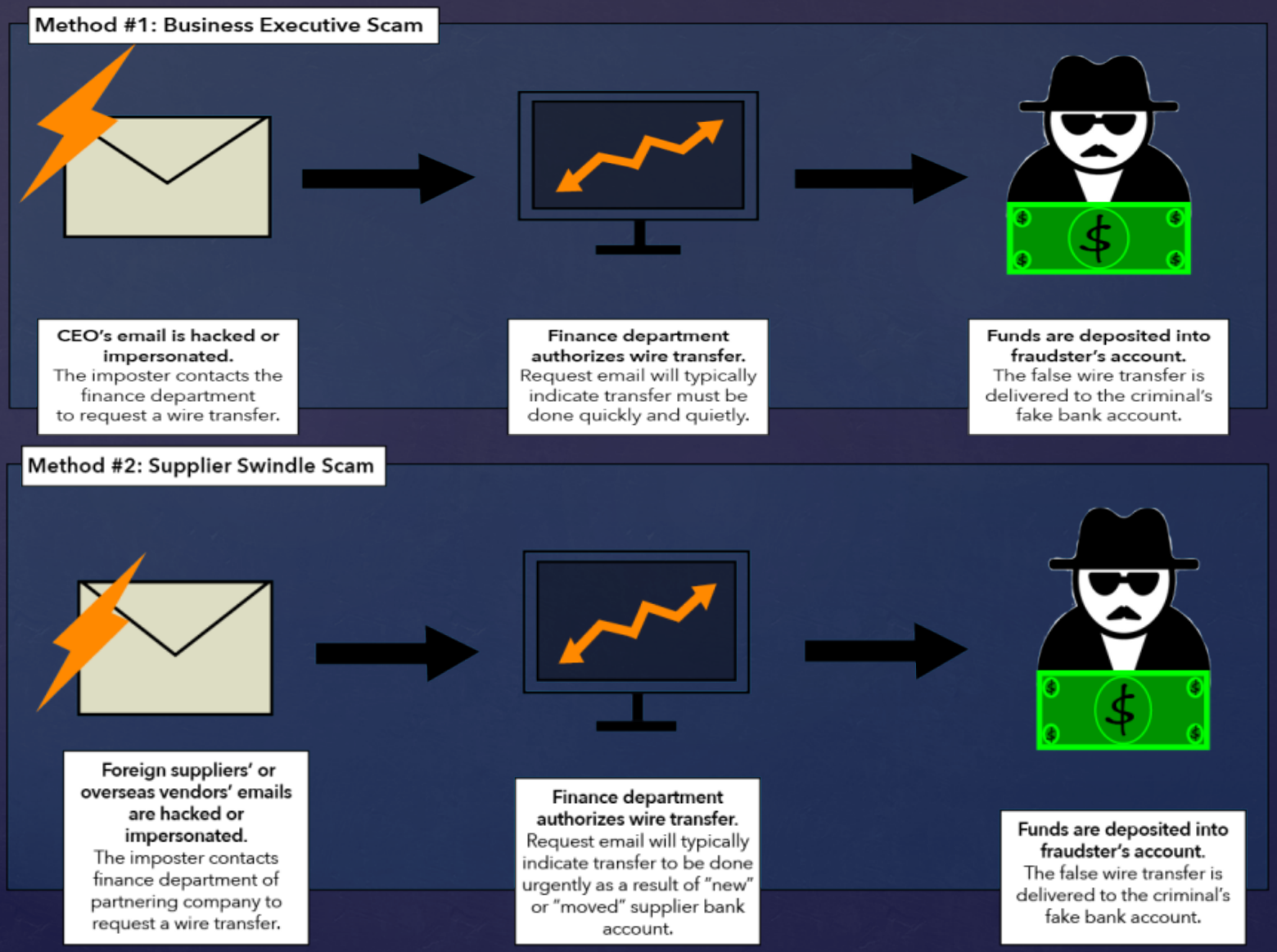
Account Takeover

- Victim unknowingly installs software by clicking on a link or visiting an infected Internet site.
- Victim logs on to their Online Banking
- Fraudsters Collect Login Credentials
- Fraudsters wait for the right time and then depending on your controls – they login after hours or if you are utilizing a token they wait until you enter your code and then they hijack the session and send you a message that Online Banking is temporarily unavailable.

DDoS Attack


1
Hacker
Distributed Denial of Service (DDoS) Attack
Zombie computer
2
Zombie computer
Zombie computer
Reflector
Reflector
Reflector
Reflector
Reflector
Reflector
Reflector
Reflector
3
4
Target

Business Email Compromise



Source: http://www.business2community.com/cybersecurity/stay-top-business-email-compromise-01595175#bQXY3U2sCwFvcKlI.97

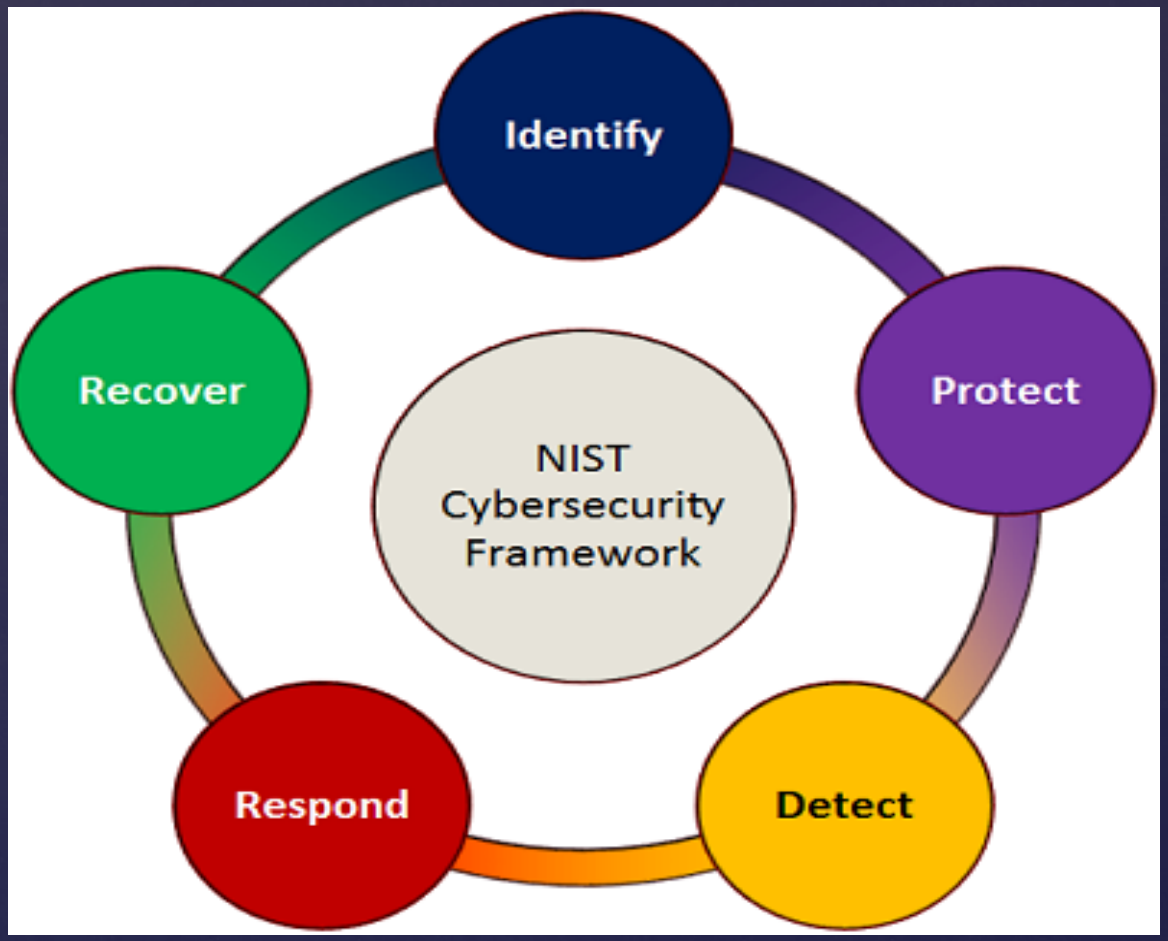
The Bottom Line…

Why should cybersecurity be important to you?

- Reputational Risk
- Legal Risk
- Financial Risk
- Strategic Risk
- Compliance Risk

The damage to companies in terms of consumer confidence, public image, and legal trouble from such incidents can be considerable, but nowhere are the effects of cybercrime more dangerous than in finance, where highly sensitive information, large sums of money, and people's livelihoods can be jeopardized.

Cybersecurity Framework



Identify

- What "information" you process?
  - Personally Identifiable Information (PPI)??
  - Financial Data?
  - Proprietary Information (trade secrets)?

Protect

- How do you keep people from stealing your information?
  - What types of computer security do you have in place?
  - Is your physical security strong?
  - What are your computer/network controls for your computer users?

Detect

- How do we know when someone has accessed our information?

Respond

- Our information has been compromised, what now?
- Who do we call?
- What should we do?

Recover
(aka The Aftermath)

- How do we get back to “normal”?
- Insurance?
- Reputation – Customer Confidence?
- Lessons Learned

- Train employees in security principles.
- Establish security practices and policies to protect sensitive information.
- Protect information, computers, and networks from cyber attacks.
- Provide firewall security for your Internet connection.
- Create a mobile device action plan.
- Make backup copies of important business data and information.

Cybersecurity Tips

- Control physical access to your computers and create user accounts for each employee.
- Secure your Wi-Fi networks.
- Employ best practice on payment cards.
- Limit employee access to data and information, and limit authority to install software.
- Passwords and authentication.
- Protect all pages on your public-facing websites, not just the checkout and sign-up pages.

Cybersecurity Tips

Resources

Texas Department of Banking
http://www.dob.texas.gov/

Federal Financial Institutions Examination Council's (FFIEC)
www.FFIEC.gov

National Institute of Standards and Technology (NIST)
www.nist.gov

Financial Services Information Sharing and Analysis Center (FS-ISAC)
www.fsisac.com

United States Computer Emergency Readiness Team (US-CERT)
US-CERT@ncas.us-cert.gov

Question & Answer Session

CONTACT INFORMATION

Ruth Norris, CISA
Texas Department of Banking
IT Security Examiner
ruth.norris@dob.texas.gov

Leilani Lim-Villegas
Texas Department of Banking
Financial Education Coordinator
leilani.lim-villegas@dob.texas.gov