# Southeast Bankers Outreach Forum

# Cybercrime & Cybersecurity

**Date:** September 28, 2017

**Presented by:** **Tony DaSilva, AAP, CISA**

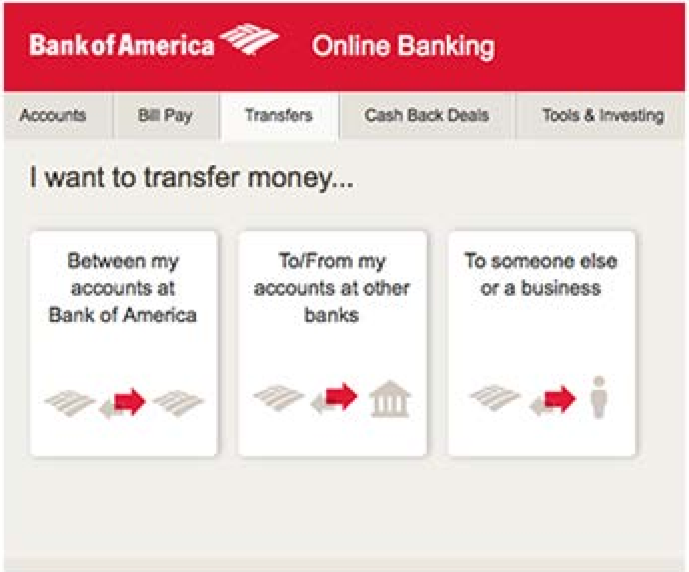
*The opinions expressed are those of the presenter and are not those of the Federal Reserve Bank of Atlanta, the Federal Reserve System, or its Board of Governors.*

FEDERAL RESERVE BANK of ATLANTA

# TOPICS

- **Electronic Banking**
- **Cybercrime**
- **Fraud**
- **Data Breaches**
- **Cybersecurity**
- **Regulatory Guidance**

# ELECTRONIC BANKING



Bank of America Online Banking

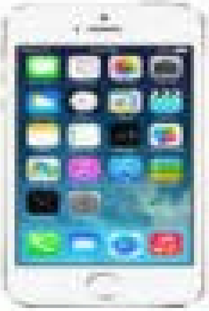
Accounts | Bill Pay | Transfers | Cash Back Deals | Tools & Investing

I want to transfer money...

Between my accounts at Bank of America

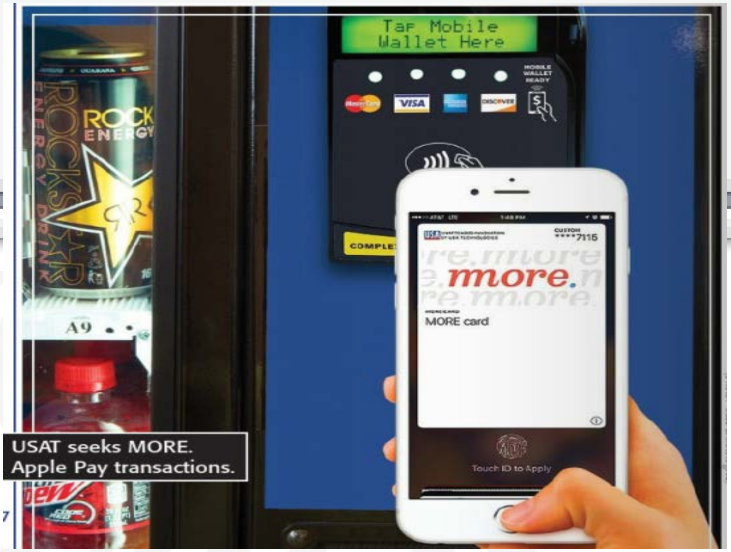
To/From my accounts at other banks

To someone else or a business



# ELECTRONIC BANKING

- Account Activity
- Internal Transfers
- Bill Pay
- RDC
- ACH
- Wire Transfer
- External Transfers
- Mobile Payments
- New Accounts



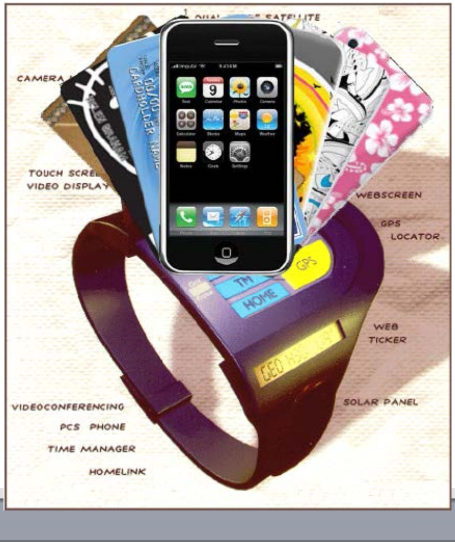
USAT seeks MORE. Apple Pay transactions.

## PAYMENT DEVICE TYPES

Device-wise, digital payments today are mainly performed with card, smartphone, tablet or PC. Joining these will be the emerging new category of wearable devices – such as smart watches and contactless wristbands.

CARD
PC
SMARTPHONE
TABLET
WEARABLE

In-car payments: Who'll be in the driver's seat?



FIS

(NYSE: FIS)

D+H

# OPPORTUNITY!

## *FOR COMMUNITY BANKS*

EBANQ

Automated Systems, Inc

NexorONE

jack henry & ASSOCIATES INC.

TEMENOS

fiserv.

# *OPPORTUNITY !*

# CYBERCRIME

**Cybercrime is a well-funded, organized business with sophisticated technology.  It is driven by a powerful combination of actors ranging from organized crime, nation states, and decentralized cyber gangs. They executed recent massive credit card and identity data breaches, using this data to profit from all types of fraud—card not present, account takeover, and new account creation–across all businesses across all regions.**

# CYBERCRIME – WHERE & WHY?

- **Where do cyber attacks come from?**

- **What is the motivation?**
  - **Ideology – making a political statement**
  - **Extortion – demand for payment to avoid website attack**
  - **Competition – disrupt a competitors online services**
  - **Fraud – used as a tool to aid in unauthorized financial gain**

# TRENDS

# THREATS & CONSEQUENCES

- **Third Party, Vendor, and Cloud**
- **Malware**
- **Ransomware**
- **Data Corruption**
- **Data Destruction**
- **Distributed Denial of Service (DDoS)**
- **Payment Account Takeovers**
- **Mobile Application Vulnerabilities**
- **Social Engineering**

# ONGOING CONCERNS

- Bank service providers as continued targets ✓

- Overload of key service providers attempting to mitigate the effects of DDoS attacks ✓

- Attacks moving down to banks of lower asset size with potentially less capability for managing the attacks ✓

- DDoS attacks being used as a diversion while fraudulent wire transfers are being transmitted (and other fraudulent/malicious transactions) ✓

# PAYMENTS CYBERCRIME

## ACH & Wire Transfers

# HOW DO CYBER CRIMINALS GAIN ACCESS?

- Deception via DDoS
- Spam
- Phishing attempts
- Spoofed web pages
- Popup ads and warnings
- Malware (Trojans, worms, etc.)
- Theft (laptops, thumb drives, etc.)
- Email attachments
- Downloads
- Social mediums

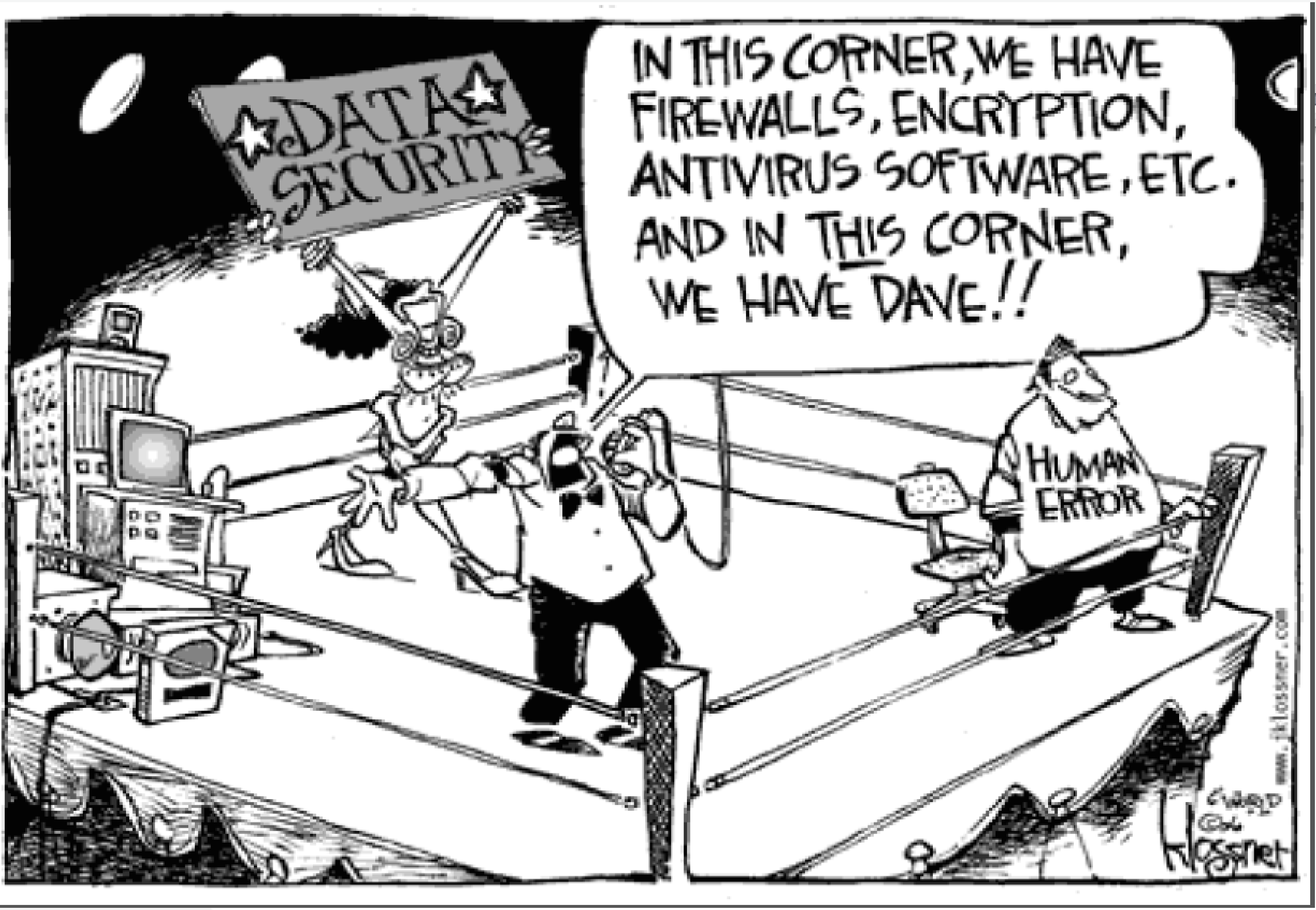
# PEOPLE THE WEAK LINK

- **Whether they come from email, the web, social media, or mobile apps, today's cyber attacks have one thing in common—they all target people.**
- **Cyber criminals have shifted tactics. Rather than relying solely on technical exploits, today's attacks fool humans into becoming unwitting accomplices, infecting systems, stealing credentials, and transferring funds.**
- **Email threats continue to plague organizations around the world, but when thinking about your defense, it's critical not to focus on malware alone. It's phishing that actually makes up the majority of threats targeting both organizations and consumers.**

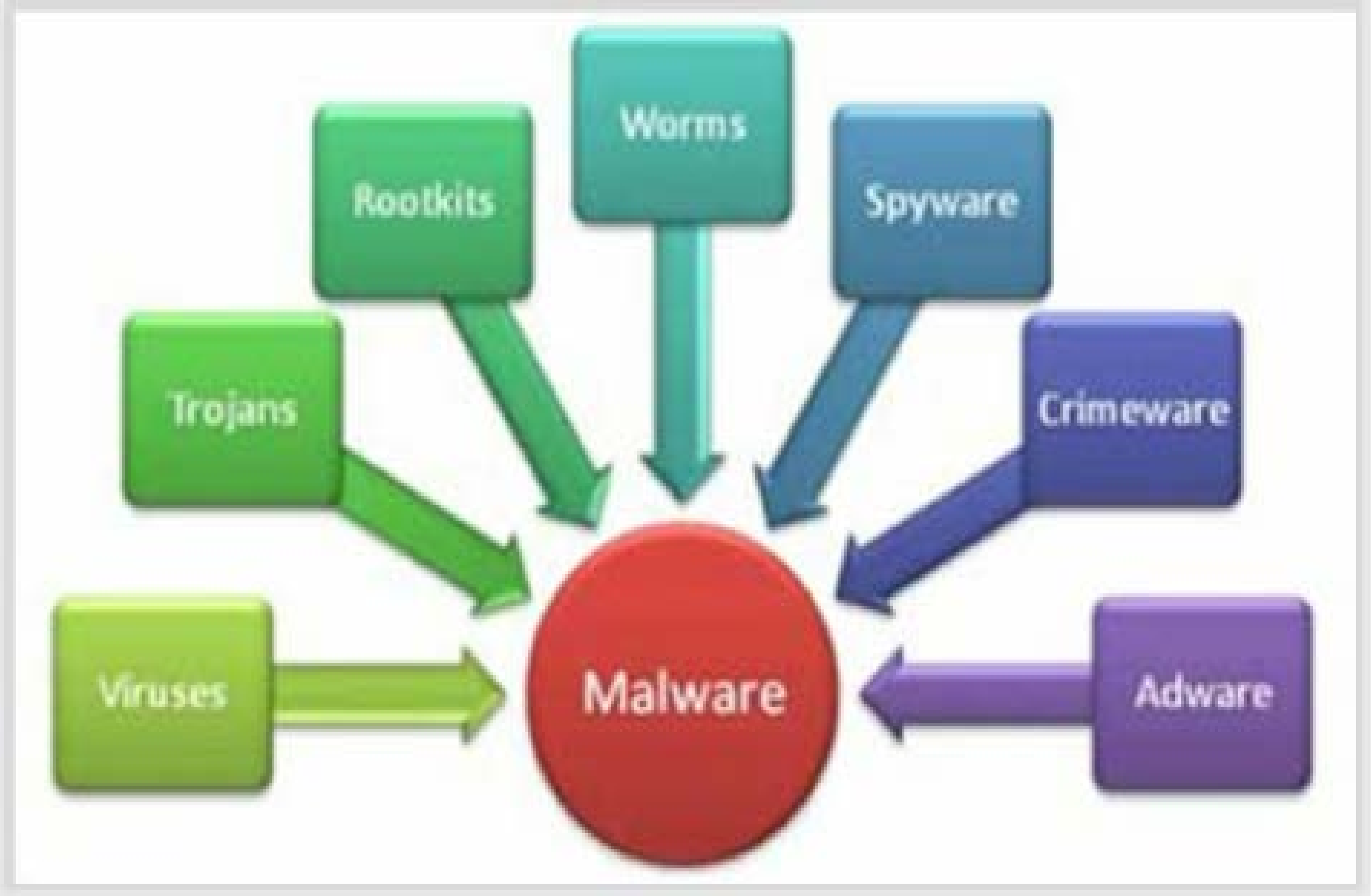
# PROTECT THE BANK

**From:**

- **Vendors**
- **Customers**
- **Employees**


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©2004 klossner

# MALWARE


Worms
Rootkits
Spyware
Trojans
Crimeware
Viruses
Malware
Adware

# JUST A FEW EXAMPLES

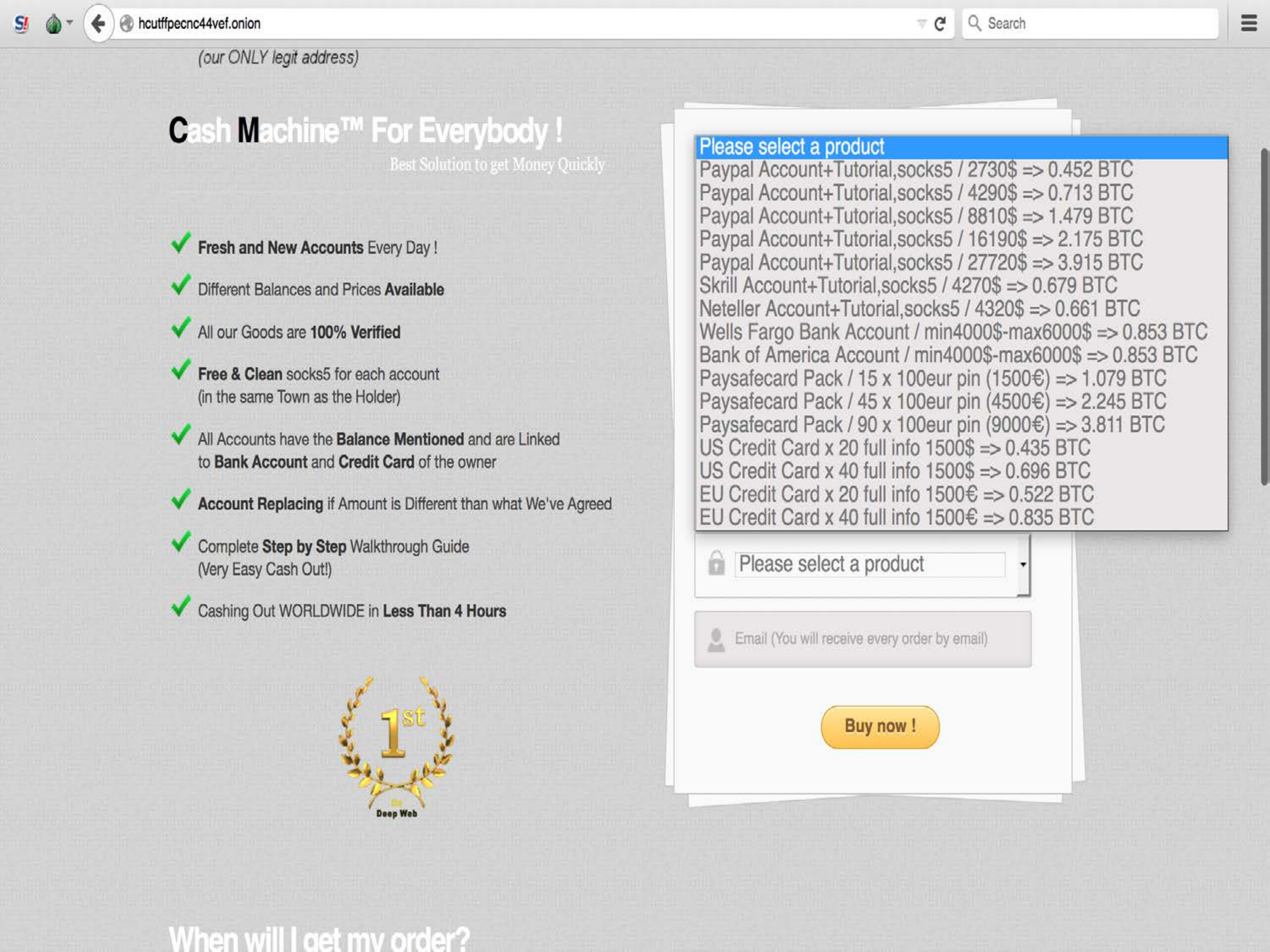
- **SpyEye– A Zeus variant that "wakes-up" and steals credentials in real time.**
- **OddJob–Keeps online sessions open after logout by the user**
- **Tatanga– Caused a screen freeze or displays a "please wait" message as it conducts transactions in the background.**
- **Zeus Mitmo– Steals SMS one-time passwords via social engineering. Can utilize smishing to get user to download malware that forwards SMS messages**
- **Ramnit Worm – It was paired with source code from the Zeus botnet, and began targeting financial institution and has the ability to "bypass two-factor authentication and transaction signing systems."**

# Dark Web

THE TOR DARK WEB MAY BE REFERRED TO AS ONIONLAND.

# TOR

**Tor is free software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router". Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult for Internet activity to be traced back to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms".**



(our ONLY legit address)

# Cash Machine™ For Everybody !

Best Solution to get Money Quickly

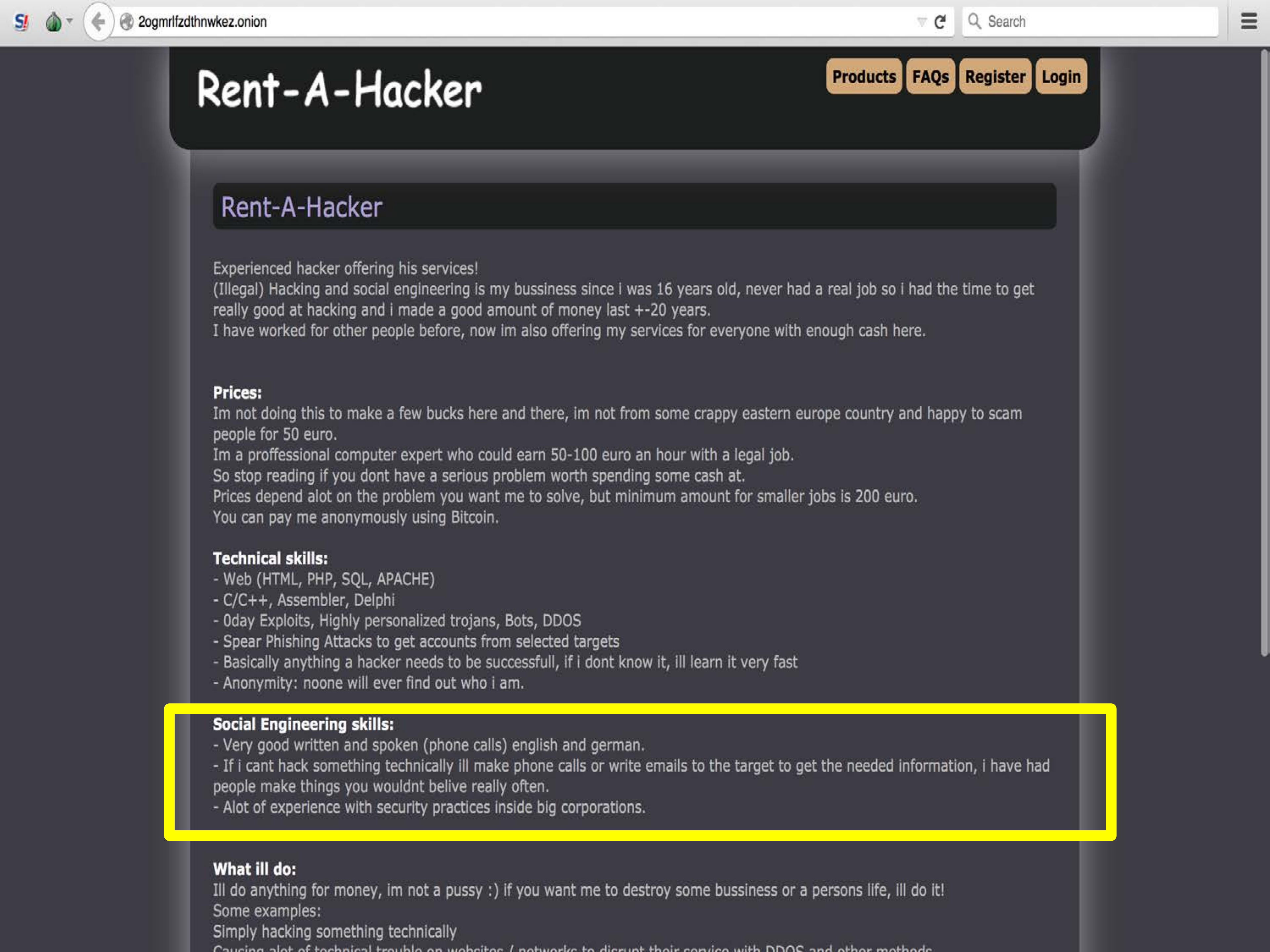
- ✓ **Fresh and New Accounts** Every Day !
- ✓ Different Balances and Prices **Available**
- ✓ All our Goods are **100% Verified**
- ✓ **Free & Clean** socks5 for each account (in the same Town as the Holder)
- ✓ All Accounts have the **Balance Mentioned** and are Linked to **Bank Account** and **Credit Card** of the owner
- ✓ **Account Replacing** if Amount is Different than what We've Agreed
- ✓ Complete **Step by Step** Walkthrough Guide (Very Easy Cash Out!)
- ✓ Cashing Out WORLDWIDE in **Less Than 4 Hours**

Please select a product
Paypal Account+Tutorial,socks5 / 2730$ => 0.452 BTC
Paypal Account+Tutorial,socks5 / 4290$ => 0.713 BTC
Paypal Account+Tutorial,socks5 / 8810$ => 1.479 BTC
Paypal Account+Tutorial,socks5 / 16190$ => 2.175 BTC
Paypal Account+Tutorial,socks5 / 27720$ => 3.915 BTC
Skrill Account+Tutorial,socks5 / 4270$ => 0.679 BTC
Neteller Account+Tutorial,socks5 / 4320$ => 0.661 BTC
Wells Fargo Bank Account / min4000$-max6000$ => 0.853 BTC
Bank of America Account / min4000$-max6000$ => 0.853 BTC
Paysafecard Pack / 15 x 100eur pin (1500€) => 1.079 BTC
Paysafecard Pack / 45 x 100eur pin (4500€) => 2.245 BTC
Paysafecard Pack / 90 x 100eur pin (9000€) => 3.811 BTC
US Credit Card x 20 full info 1500$ => 0.435 BTC
US Credit Card x 40 full info 1500$ => 0.696 BTC
EU Credit Card x 20 full info 1500€ => 0.522 BTC
EU Credit Card x 40 full info 1500€ => 0.835 BTC

Please select a product

Email (You will receive every order by email)

## When will I get my order?



# Rent-A-Hacker

## Rent-A-Hacker

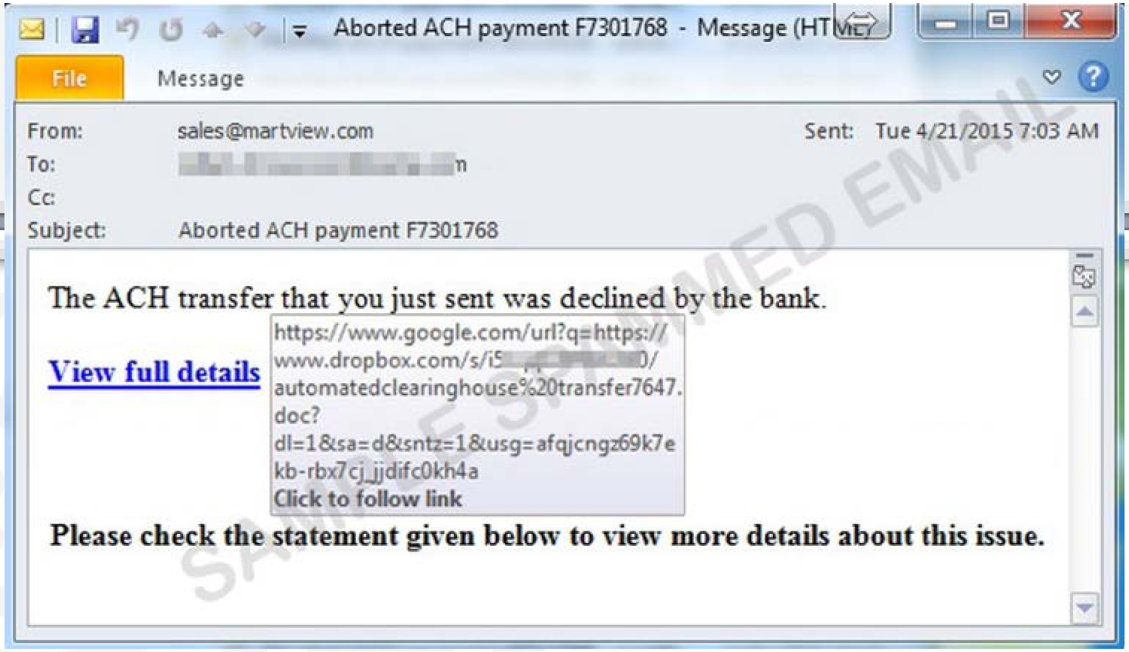
Experienced hacker offering his services!
(Illegal) Hacking and social engineering is my bussiness since i was 16 years old, never had a real job so i had the time to get really good at hacking and i made a good amount of money last +-20 years.
I have worked for other people before, now im also offering my services for everyone with enough cash here.

**Prices:**
Im not doing this to make a few bucks here and there, im not from some crappy eastern europe country and happy to scam people for 50 euro.
Im a proffessional computer expert who could earn 50-100 euro an hour with a legal job.
So stop reading if you dont have a serious problem worth spending some cash at.
Prices depend alot on the problem you want me to solve, but minimum amount for smaller jobs is 200 euro.
You can pay me anonymously using Bitcoin.

**Technical skills:**
- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets
- Basically anything a hacker needs to be successfull, if i dont know it, ill learn it very fast
- Anonymity: noone will ever find out who i am.

**Social Engineering skills:**
- Very good written and spoken (phone calls) english and german.
- If i cant hack something technically ill make phone calls or write emails to the target to get the needed information, i have had people make things you wouldnt belive really often.
- Alot of experience with security practices inside big corporations.

**What ill do:**
Ill do anything for money, im not a pussy :) if you want me to destroy some bussiness or a persons life, ill do it!
Some examples:
Simply hacking something technically
Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods



From: sales@martview.com

Sent: Tue 4/21/2015 7:03 AM

To: [redacted]

Cc:

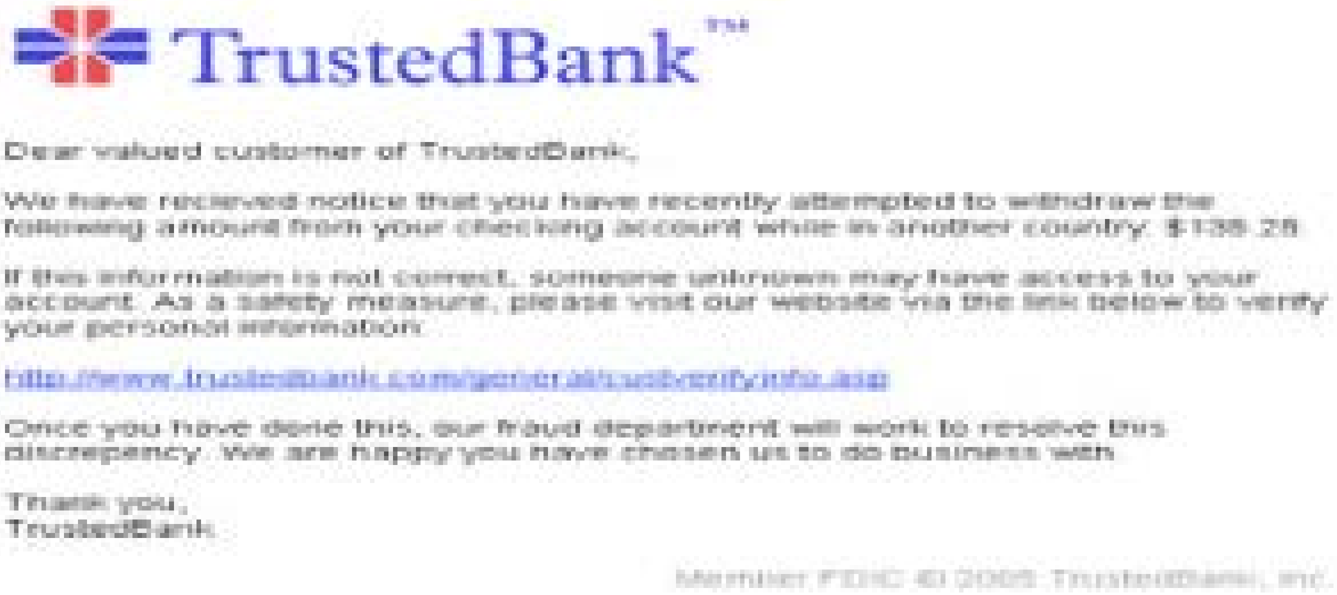
Subject: Aborted ACH payment F7301768

The ACH transfer that you just sent was declined by the bank.

**View full details**

https://www.google.com/url?q=https://www.dropbox.com/s/i5[redacted]0/automatedclearinghouse%20transfer7647.doc?dl=1&sa=d&sntz=1&usg=afqjcngz69k7ekb-rbx7cj_jjdifc0kh4a
Click to follow link

**Please check the statement given below to view more details about this issue.**



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information.

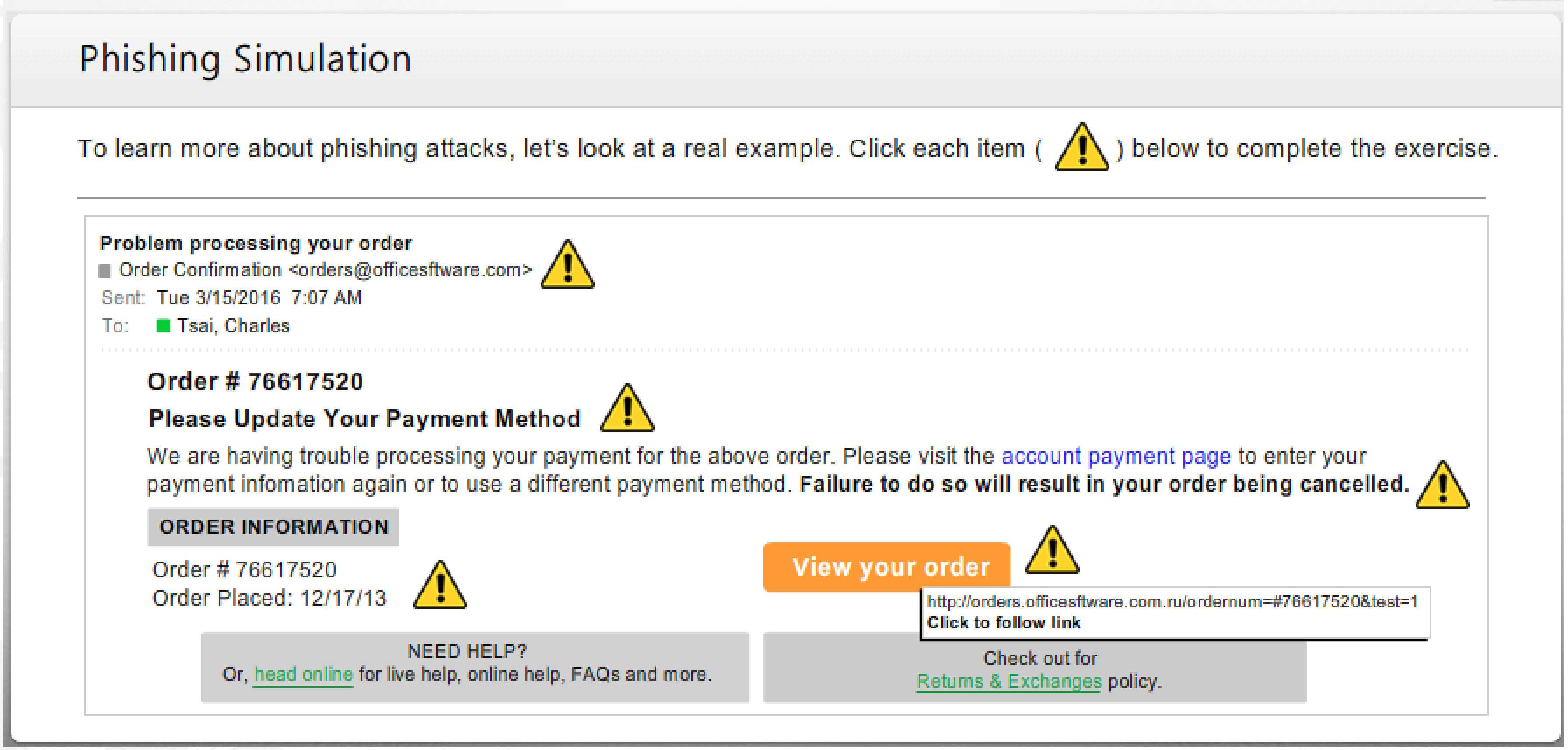
http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

# PHISHING



## Phishing Simulation

To learn more about phishing attacks, let's look at a real example. Click each item ( ⚠ ) below to complete the exercise.

**Problem processing your order**
Order Confirmation <orders@officesftware.com> ⚠
Sent: Tue 3/15/2016 7:07 AM
To: 🟩 Tsai, Charles

**Order # 76617520**

**Please Update Your Payment Method** ⚠

We are having trouble processing your payment for the above order. Please visit the account payment page to enter your payment infomation again or to use a different payment method. **Failure to do so will result in your order being cancelled.** ⚠

**ORDER INFORMATION**

Order # 76617520
Order Placed: 12/17/13 ⚠

⚠

http://orders.officesftware.com.ru/ordernum=#76617520&test=1
**Click to follow link**

NEED HELP?
Or, head online for live help, online help, FAQs and more.

Check out for
Returns & Exchanges policy.

# VAWTRAK

- **Banking malware strain known as Vawtrak, which compromises commonly used URLs by injecting them with code. This allows the hackers to steal online banking credentials as they are input on the bank's website.**
- **Vawtrak ranks as the "single most dangerous threat" among botnet-based cybercrime malware strains on the market today.**
- **While Vawtrak's crimeware-as-a-service model, better known as CaaS, has been around since about 2006, researchers say the crime rings that manage this type of service have perfected their techniques, affording them the ability to adapt their attacks for specific targets.**
- **Some of the most notable U.S. banking institutions that have been targeted by this attack so far include Bank of America, Wells Fargo, Capital One Financial Corp., Citigroup and JPMorgan Chase.**

BANK INFO SECURITY®

# RANSOMWARE

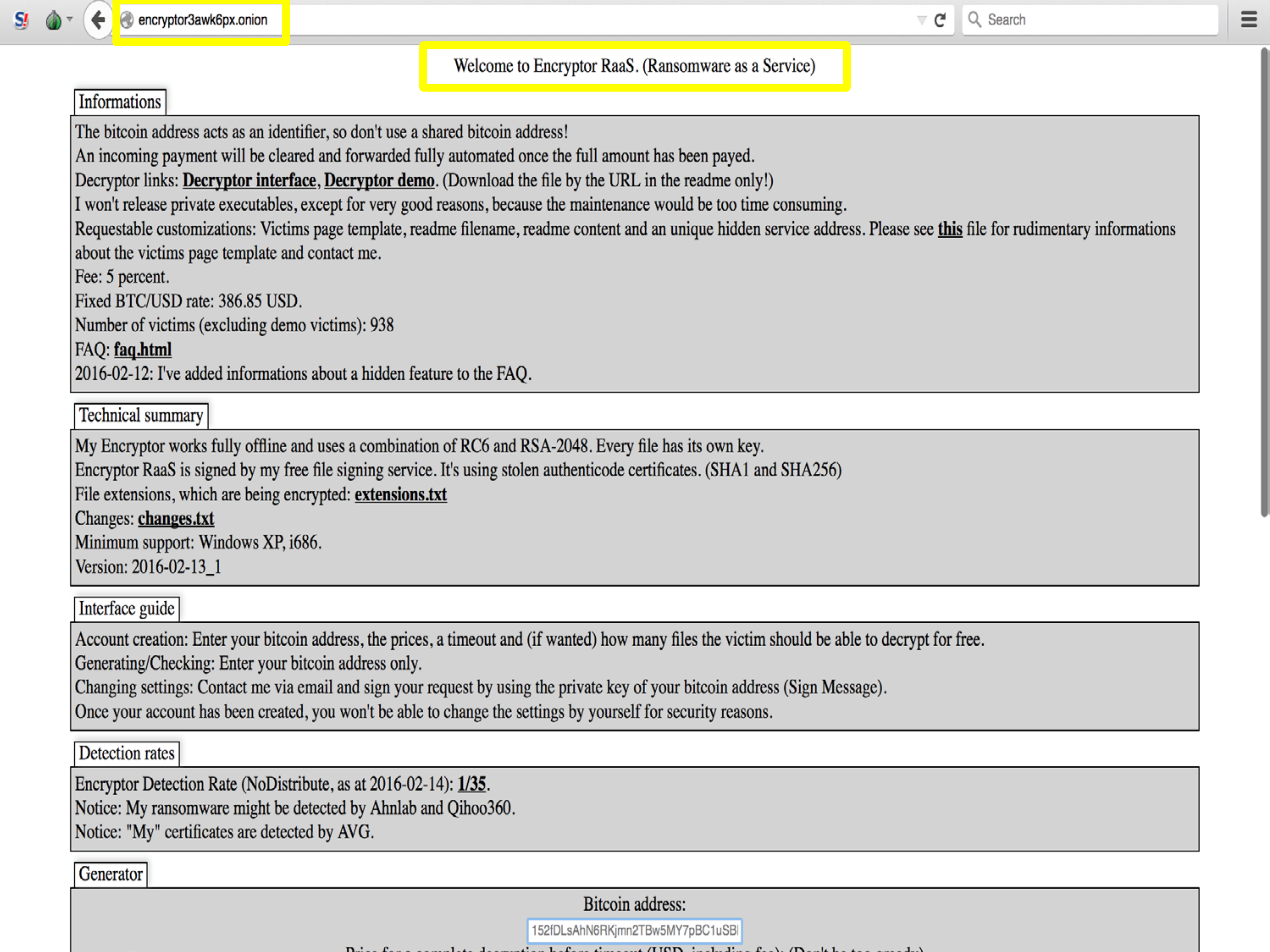
**Ransomware can:**

- **Prevent you from accessing Windows.**
- **Encrypt files so you can't use them.**
- **Stop certain apps from running (like your web browser).**
- **Ransomware will demand that you pay money (a “ransom”) to get access to your PC or files. We have also seen them make you complete surveys.**
- **There is no guarantee that paying the fine or doing what the ransomware tells you will give access to your PC or files again.**

## A $1 Million Ransomware Payment

South Korean web hosting firm Nayana decided to pay 1.3 billion won ($1.1 million) in ransom after its servers were infected with Erebus Ransomware on June 10. Nayana CEO Hwang Chilghong said the payment was necessary to restore 150 servers and the 3,400-plus affected client websites. If they did not pay, the CEO said, the damage would be too widespread and too many people would be impacted. However, researchers fear that the massive payment may have drawn the attention of other extortionists to South Korean businesses.

For example, shortly after the Nayana attack, a group using the Armada Collective name sent extortion messages to at least 27 Korean financial institutions threatening DDoS attacks if they didn't pay 10-15 bitcoin ($25,000 to $37,000) each. SurfWatch Labs advises against ever paying extortionists, particularly in the case of DDoS attacks, as they can be easily and repeatedly launched.



Welcome to Encryptor RaaS. (Ransomware as a Service)

Informations

The bitcoin address acts as an identifier, so don't use a shared bitcoin address!
An incoming payment will be cleared and forwarded fully automated once the full amount has been payed.
Decryptor links: **Decryptor interface**, **Decryptor demo**. (Download the file by the URL in the readme only!)
I won't release private executables, except for very good reasons, because the maintenance would be too time consuming.
Requestable customizations: Victims page template, readme filename, readme content and an unique hidden service address. Please see **this** file for rudimentary informations about the victims page template and contact me.
Fee: 5 percent.
Fixed BTC/USD rate: 386.85 USD.
Number of victims (excluding demo victims): 938
FAQ: **faq.html**
2016-02-12: I've added informations about a hidden feature to the FAQ.

Technical summary

My Encryptor works fully offline and uses a combination of RC6 and RSA-2048. Every file has its own key.
Encryptor RaaS is signed by my free file signing service. It's using stolen authenticode certificates. (SHA1 and SHA256)
File extensions, which are being encrypted: **extensions.txt**
Changes: **changes.txt**
Minimum support: Windows XP, i686.
Version: 2016-02-13_1

Interface guide

Account creation: Enter your bitcoin address, the prices, a timeout and (if wanted) how many files the victim should be able to decrypt for free.
Generating/Checking: Enter your bitcoin address only.
Changing settings: Contact me via email and sign your request by using the private key of your bitcoin address (Sign Message).
Once your account has been created, you won't be able to change the settings by yourself for security reasons.

Detection rates

Encryptor Detection Rate (NoDistribute, as at 2016-02-14): **1/35**.
Notice: My ransomware might be detected by Ahnlab and Qihoo360.
Notice: "My" certificates are detected by AVG.

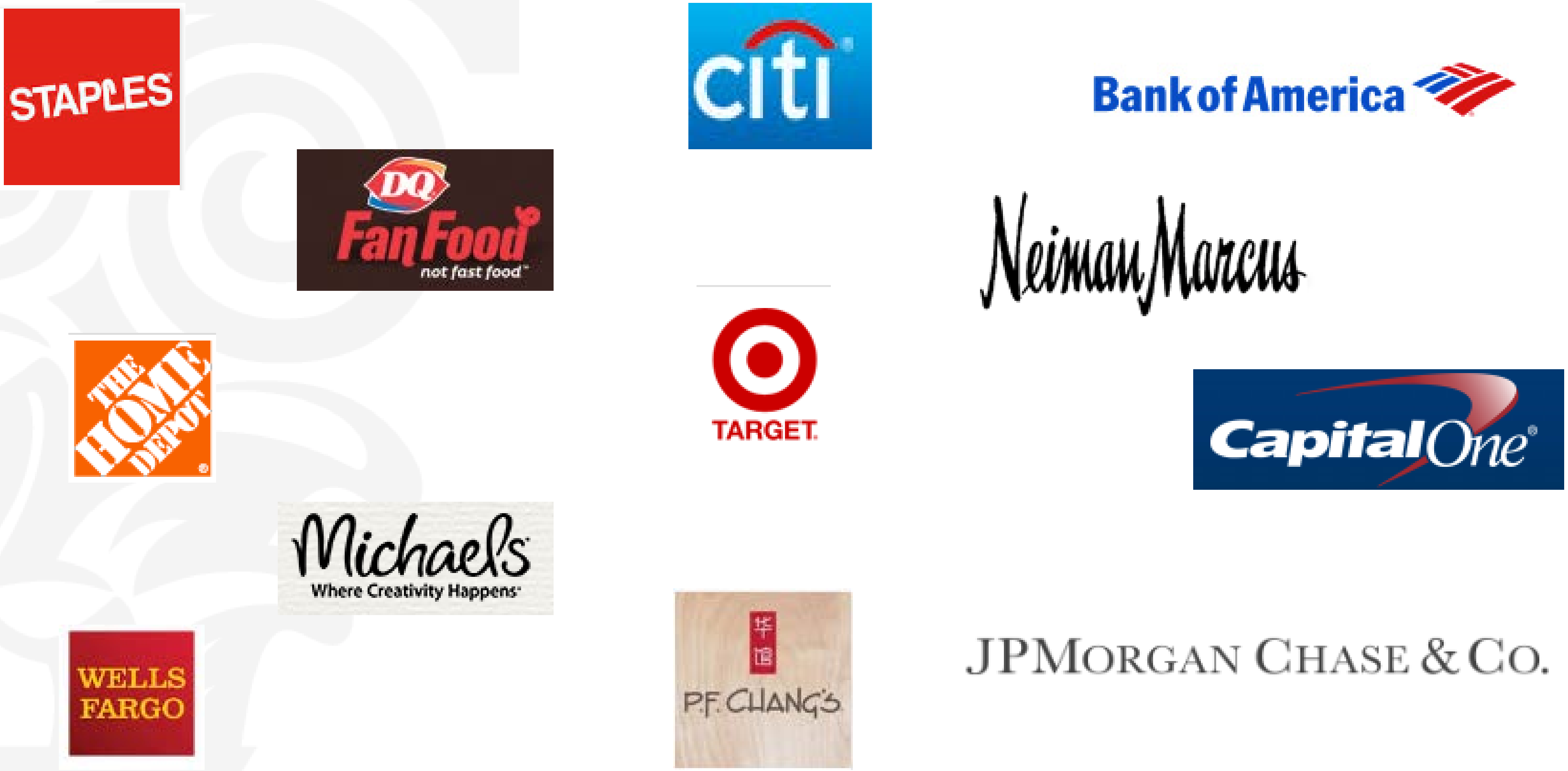
Generator

Bitcoin address:

152fDLsAhN6RKjmn2TBw5MY7pBC1uSBl

Price for a complete decryption before timeout (USD, including fee): (Don't be too greedy)

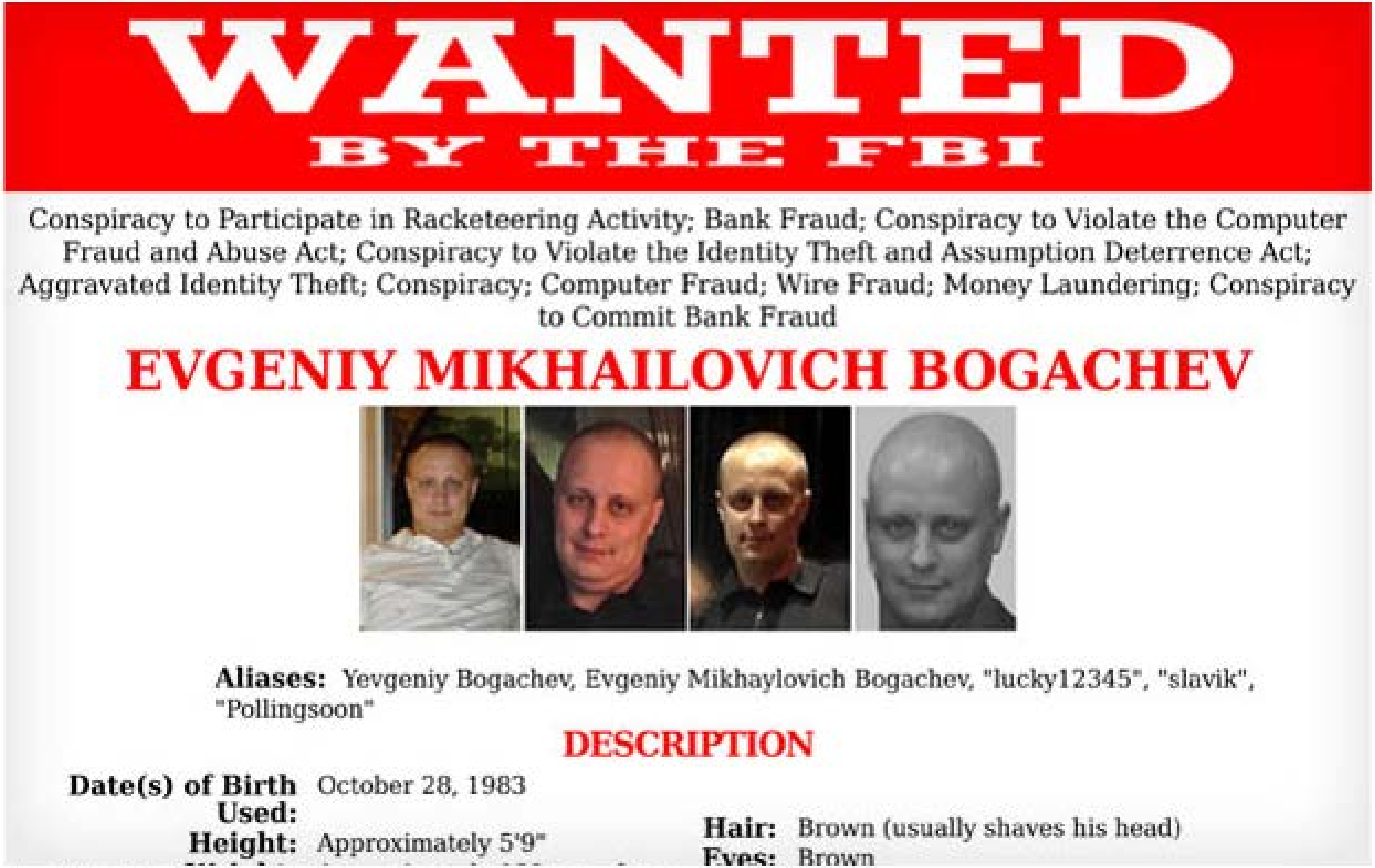
# DATA BREACHES



# WHO

- **Law enforcement agencies are all reporting a significant increase in funds transfer fraud involving the exploitation of valid online banking credentials belonging to small and medium sized businesses.**

- **Eastern European organized crimes groups are believed to be predominantly responsible for the activities that are also employing witting and unwitting accomplices in the United States (money mules) to receive, cash and forward payments from thousands to millions of dollars to overseas locations via popular money and wire transfer services.**



# WANTED

## BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

## EVGENIY MIKHAILOVICH BOGACHEV

**Aliases:** Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

## DESCRIPTION

**Date(s) of Birth Used:** October 28, 1983

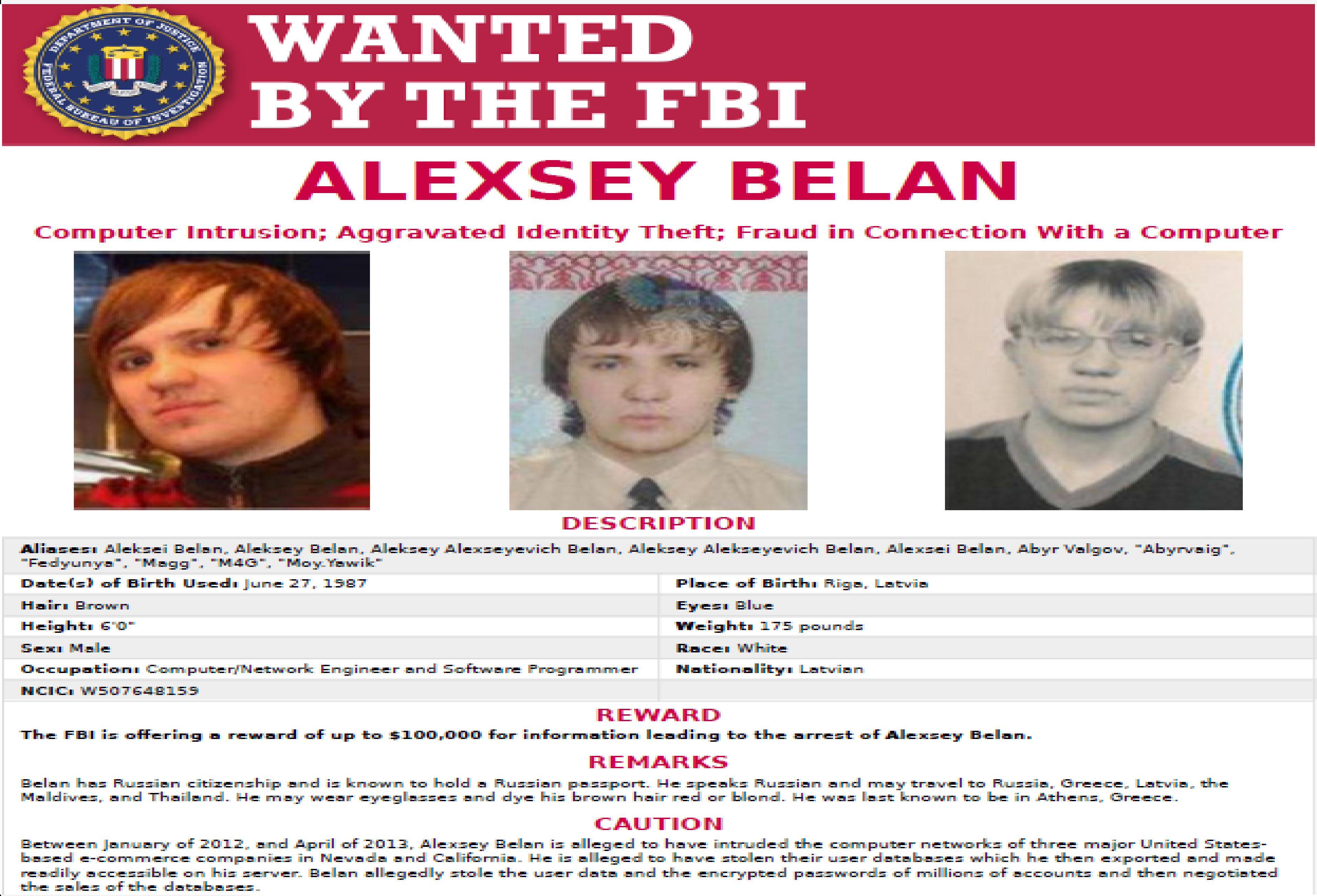
**Height:** Approximately 5'9"

**Hair:** Brown (usually shaves his head)

**Eyes:** Brown

The FBI's $3 million 'wanted' poster for Evgeniy Mikhailovich Bogachev.

How much money would it take for you to rat out a member of a Russian organized crime gang?



# WANTED BY THE FBI

## ALEXSEY BELAN

Computer Intrusion; Aggravated Identity Theft; Fraud in Connection With a Computer

### DESCRIPTION

**Aliases:** Aleksei Belan, Aleksey Belan, Aleksey Alexseyevich Belan, Aleksey Alekseyevich Belan, Alexsei Belan, Abyr Valgov, "Abyrvaig", "Fedyunya", "Magg", "M4G", "Moy.Yawik"

| | |
|---|---|
| **Date(s) of Birth Used:** June 27, 1987 | **Place of Birth:** Riga, Latvia |
| **Hair:** Brown | **Eyes:** Blue |
| **Height:** 6'0" | **Weight:** 175 pounds |
| **Sex:** Male | **Race:** White |
| **Occupation:** Computer/Network Engineer and Software Programmer | **Nationality:** Latvian |
| **NCIC:** W507648159 | |

### REWARD

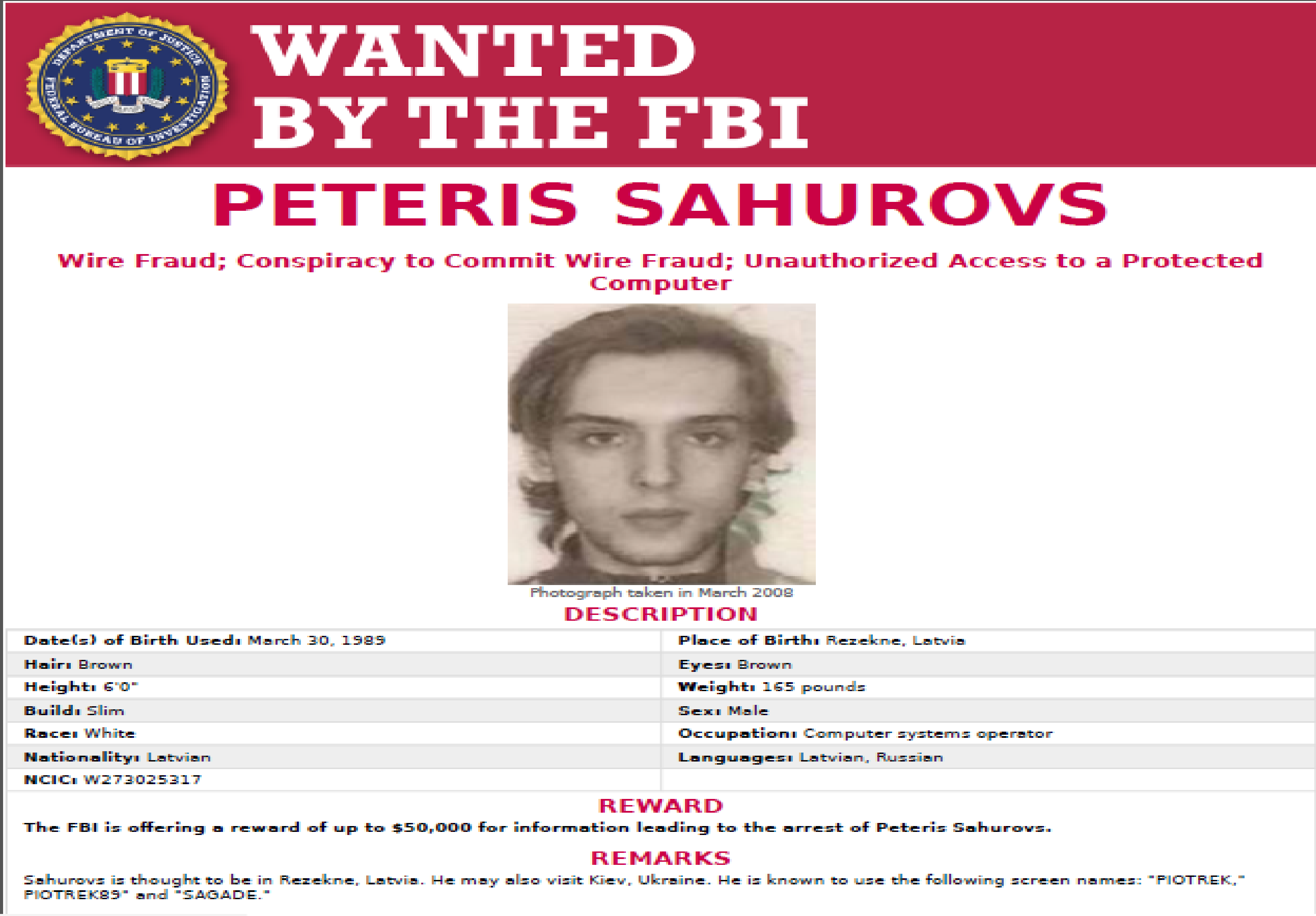
**The FBI is offering a reward of up to $100,000 for information leading to the arrest of Alexsey Belan.**

### REMARKS

Belan has Russian citizenship and is known to hold a Russian passport. He speaks Russian and may travel to Russia, Greece, Latvia, the Maldives, and Thailand. He may wear eyeglasses and dye his brown hair red or blond. He was last known to be in Athens, Greece.

### CAUTION

Between January of 2012, and April of 2013, Alexsey Belan is alleged to have intruded the computer networks of three major United States-based e-commerce companies in Nevada and California. He is alleged to have stolen their user databases which he then exported and made readily accessible on his server. Belan allegedly stole the user data and the encrypted passwords of millions of accounts and then negotiated the sales of the databases.



# WANTED BY THE FBI

## PETERIS SAHUROVS

Wire Fraud; Conspiracy to Commit Wire Fraud; Unauthorized Access to a Protected Computer

Photograph taken in March 2008

### DESCRIPTION

| | |
|---|---|
| **Date(s) of Birth Used:** March 30, 1989 | **Place of Birth:** Rezekne, Latvia |
| **Hair:** Brown | **Eyes:** Brown |
| **Height:** 6'0" | **Weight:** 165 pounds |
| **Build:** Slim | **Sex:** Male |
| **Race:** White | **Occupation:** Computer systems operator |
| **Nationality:** Latvian | **Languages:** Latvian, Russian |
| **NCIC:** W273025317 | |

### REWARD

**The FBI is offering a reward of up to $50,000 for information leading to the arrest of Peteris Sahurovs.**

### REMARKS

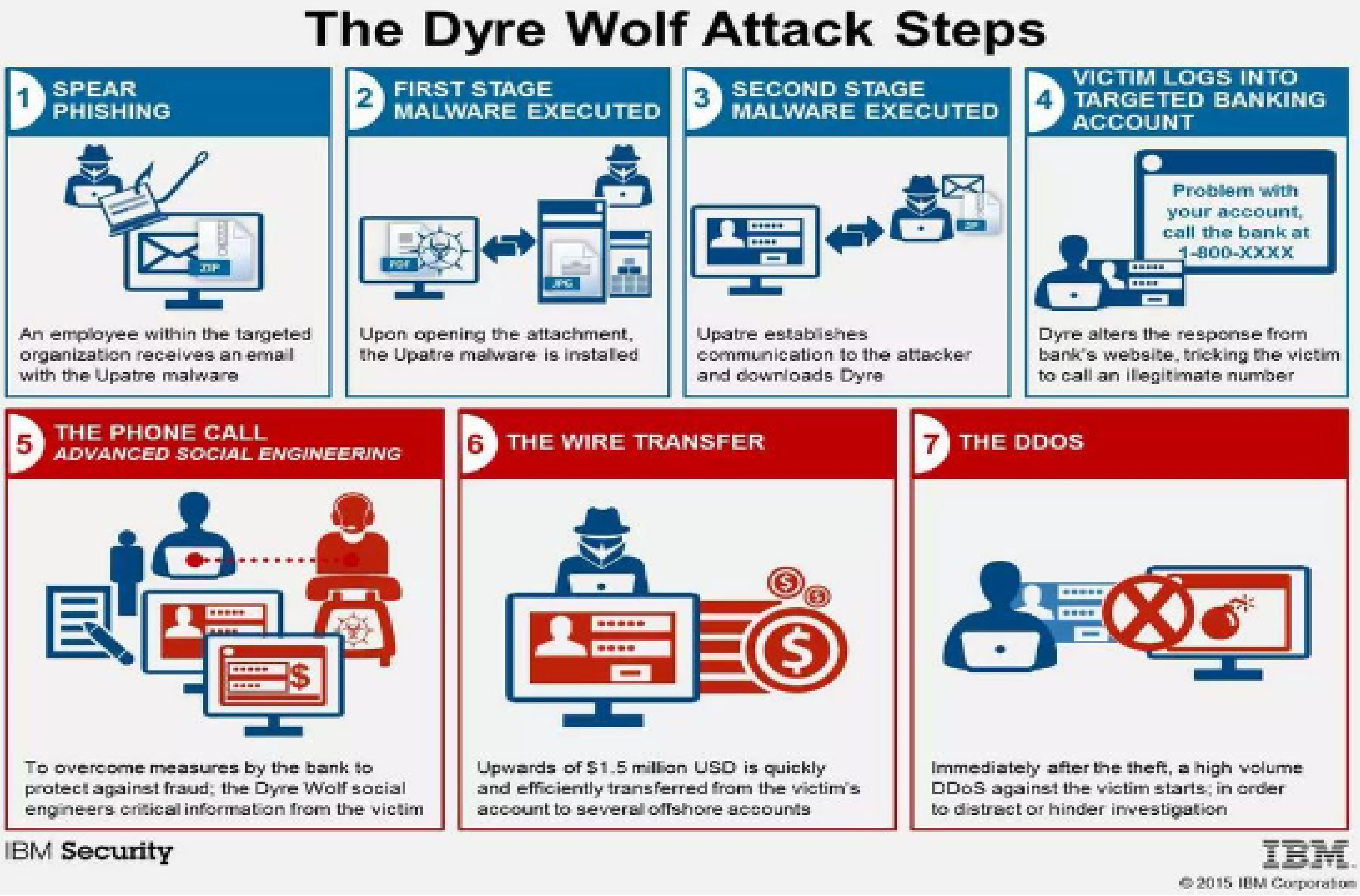
Sahurovs is thought to be in Rezekne, Latvia. He may also visit Kiev, Ukraine. He is known to use the following screen names: "PIOTREK," PIOTREK89" and "SAGADE."

# $1 MILLION STOLEN

**IBM senior threat researcher John Kuhn, notes that The Dyre Wolf malware has been used to steal more than $1 million from businesses within one month.**

**What's so concerning about attacks waged with The Dyre Wolf malware is that they involve sophisticated social engineering and, in some cases, even distributed-denial-of-service attacks, security experts say.**

***It's also clear, they say, that the fraudsters behind The Dyre Wolf malware attacks are extremely knowledgeable about banking institutions' back-end systems and online-banking platforms.***



# The Dyre Wolf Attack Steps

## 1 SPEAR PHISHING

An employee within the targeted organization receives an email with the Upatre malware

## 2 FIRST STAGE MALWARE EXECUTED

Upon opening the attachment, the Upatre malware is installed

## 3 SECOND STAGE MALWARE EXECUTED

Upatre establishes communication to the attacker and downloads Dyre

## 4 VICTIM LOGS INTO TARGETED BANKING ACCOUNT

Dyre alters the response from bank's website, tricking the victim to call an illegitimate number

## 5 THE PHONE CALL *ADVANCED SOCIAL ENGINEERING*

To overcome measures by the bank to protect against fraud; the Dyre Wolf social engineers critical information from the victim

## 6 THE WIRE TRANSFER

Upwards of $1.5 million USD is quickly and efficiently transferred from the victim's account to several offshore accounts

## 7 THE DDOS

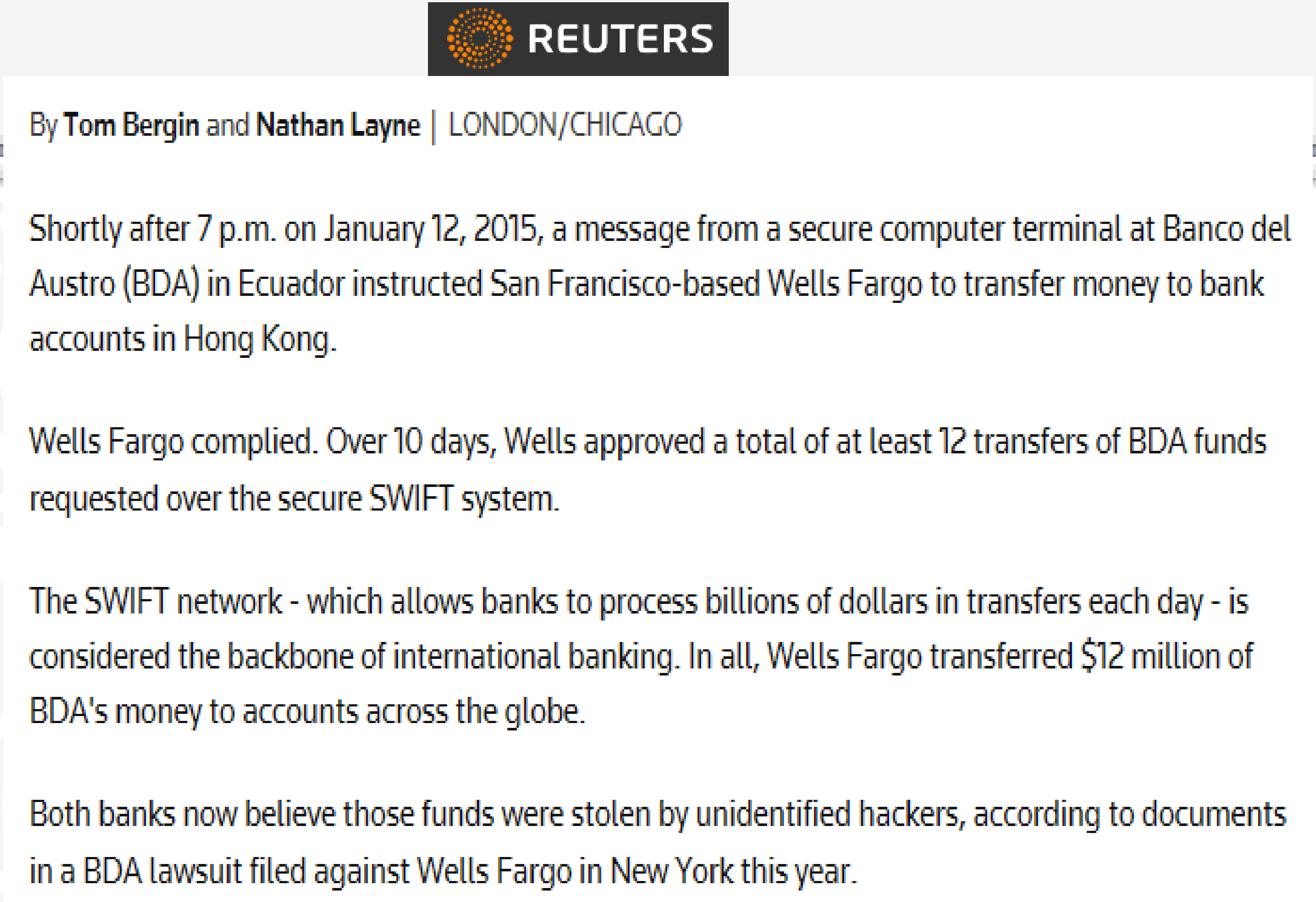
Immediately after the theft, a high volume DDoS against the victim starts; in order to distract or hinder investigation

IBM Security

IBM

# Special Report: Cyber thieves exploit banks' faith in SWIFT transfer network

Society for Worldwide
Interbank Financial
Telecommunication



REUTERS

By **Tom Bergin** and **Nathan Layne** | LONDON/CHICAGO

Shortly after 7 p.m. on January 12, 2015, a message from a secure computer terminal at Banco del Austro (BDA) in Ecuador instructed San Francisco-based Wells Fargo to transfer money to bank accounts in Hong Kong.

Wells Fargo complied. Over 10 days, Wells approved a total of at least 12 transfers of BDA funds requested over the secure SWIFT system.

The SWIFT network - which allows banks to process billions of dollars in transfers each day - is considered the backbone of international banking. In all, Wells Fargo transferred $12 million of BDA's money to accounts across the globe.

Both banks now believe those funds were stolen by unidentified hackers, according to documents in a BDA lawsuit filed against Wells Fargo in New York this year.

# 2016 BANGLADESH BANK HEIST

**In February 2016, instructions to steal US$951 million from Bangladesh Bank, the central bank of Bangladesh, were issued via the SWIFT network. Five transactions issued by hackers, worth $101 million and withdrawn from a Bangladesh Bank account at the Federal Reserve Bank of New York, succeeded, with $20 million traced to Sri Lanka (since recovered) and $81 million to the Philippines (about $18 million recovered). The Federal Reserve Bank of NY blocked the remaining thirty transactions, amounting to $850 million, at the request of Bangladesh Bank. It was identified later that Dridex malware was used for the attack.**

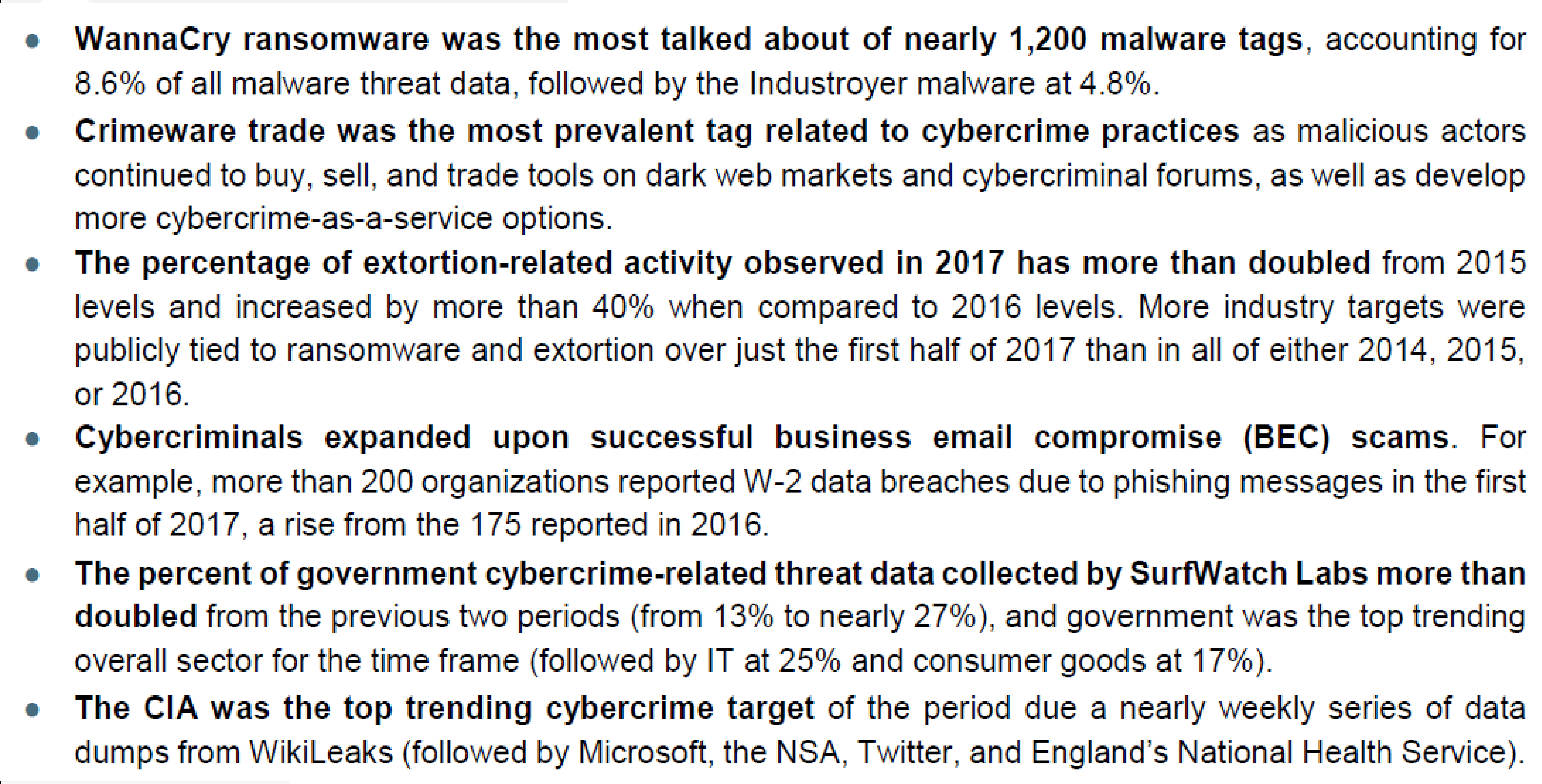
# DRIDEX

Investigators have linked malware used by Russian and eastern European cyber gangs to a string of bank heists that culminated in the record-breaking theft of US$81 million from Bangladesh's central bank. The gangs operate in Russia and former parts of the Soviet Union, including Moldova and Kazakhstan.

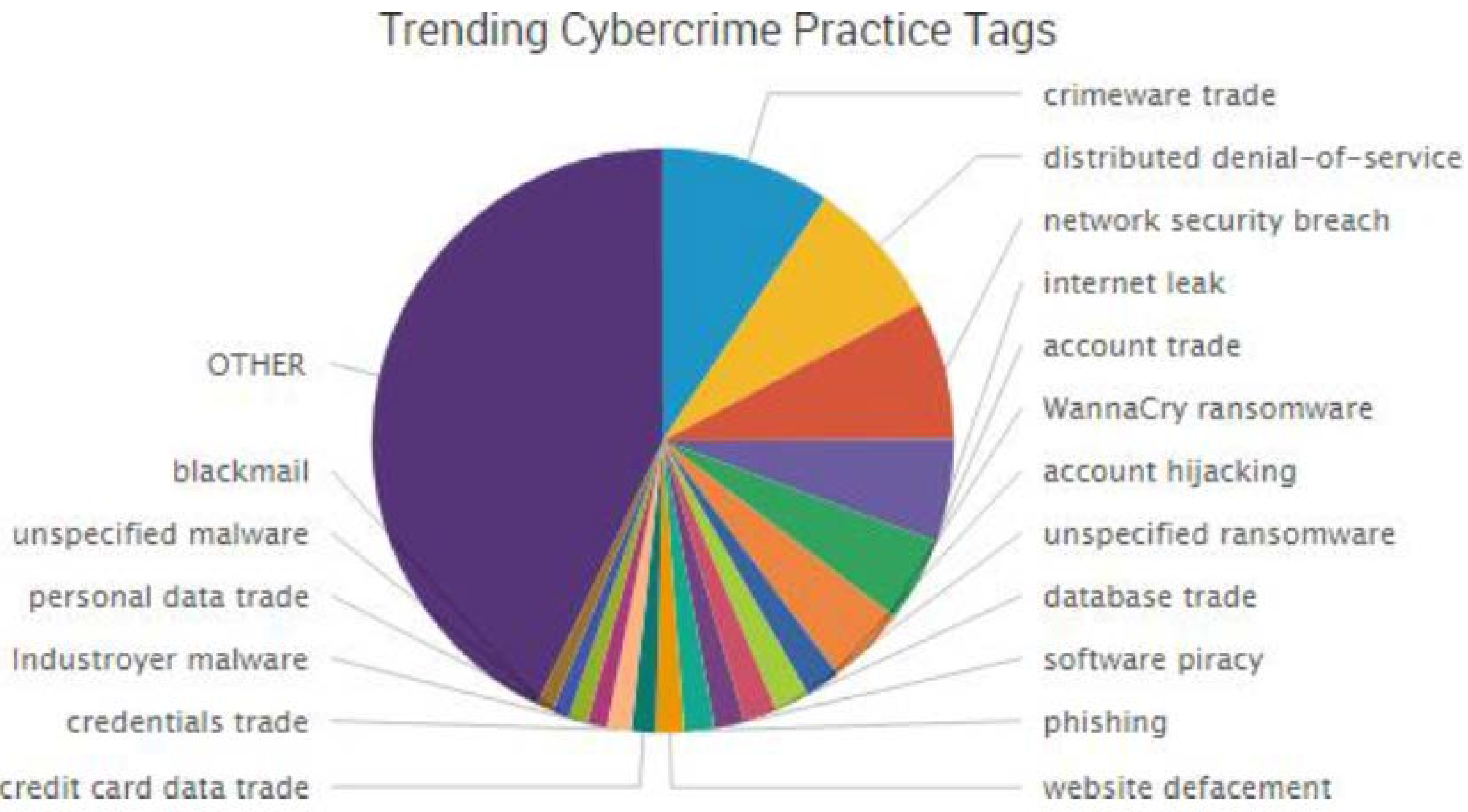
Dridex, which is used to identify the malware and the group that uses it, is spread through e-mail that infiltrate computers and harvest information like user names and passwords which are used to gain access to privileged networks.

First spotted in 2014, Dridex is one of the most serious online threats facing consumers and businesses, said security firm Symantec. The disciplined and highly organized gang behind the malware operates in many ways like an ordinary company, following a Monday-to-Friday work week and even taking time off for Christmas.

# FIRST HALF 2017



- **WannaCry ransomware was the most talked about of nearly 1,200 malware tags**, accounting for 8.6% of all malware threat data, followed by the Industroyer malware at 4.8%.
- **Crimeware trade was the most prevalent tag related to cybercrime practices** as malicious actors continued to buy, sell, and trade tools on dark web markets and cybercriminal forums, as well as develop more cybercrime-as-a-service options.
- **The percentage of extortion-related activity observed in 2017 has more than doubled** from 2015 levels and increased by more than 40% when compared to 2016 levels. More industry targets were publicly tied to ransomware and extortion over just the first half of 2017 than in all of either 2014, 2015, or 2016.
- **Cybercriminals expanded upon successful business email compromise (BEC) scams**. For example, more than 200 organizations reported W-2 data breaches due to phishing messages in the first half of 2017, a rise from the 175 reported in 2016.
- **The percent of government cybercrime-related threat data collected by SurfWatch Labs more than doubled** from the previous two periods (from 13% to nearly 27%), and government was the top trending overall sector for the time frame (followed by IT at 25% and consumer goods at 17%).
- **The CIA was the top trending cybercrime target** of the period due a nearly weekly series of data dumps from WikiLeaks (followed by Microsoft, the NSA, Twitter, and England’s National Health Service).

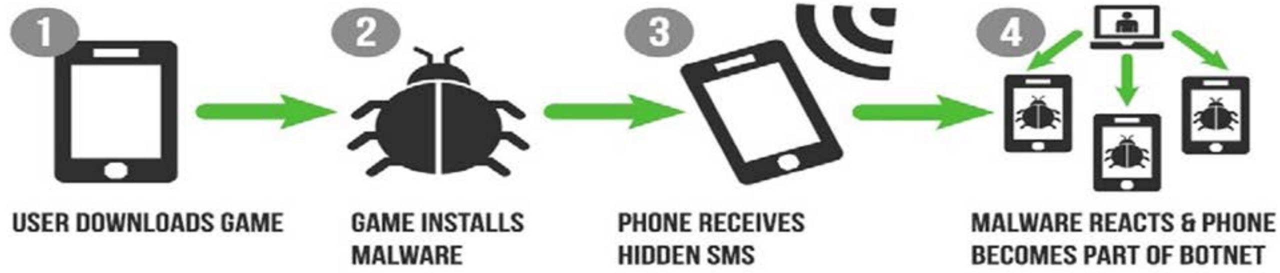


Trending Cybercrime Practice Tags

*SurfWatch Labs collected data on a wide variety of cybercrime practices, including both public attacks and dark web activity, in the first half of 2017.*

# THE NEXT RISK: MOBILE MALWARE

- **Mobile malware has been growing in popularity:**
  - Primarily targets Android platform.
  - Some early attacks were against BlackBerry.
- **Malware for attacker financial gain:**
  - Simple message service (SMS) to premium-rate-short code, bills victim (up to $50/message).
  - Zeus Trojan intercepts SMS messages for banking authentication systems.
- **Malware for advertising delivery (search engine poisoning)**
- **Malware for location tracking and piracy attacks**

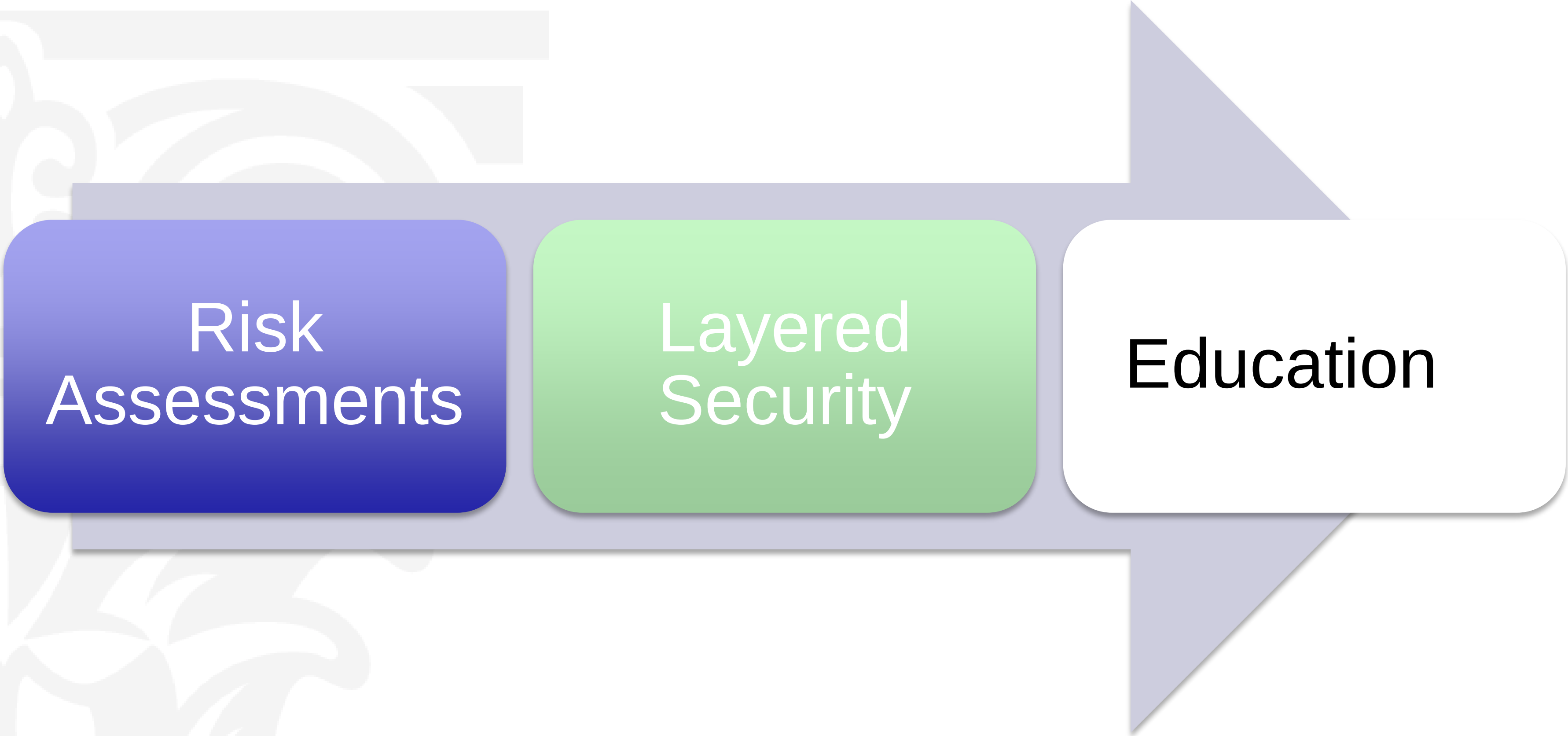

1
USER DOWNLOADS GAME
2
GAME INSTALLS MALWARE
3
PHONE RECEIVES HIDDEN SMS
4
MALWARE REACTS & PHONE BECOMES PART OF BOTNET

**Source:** Trustwave, Inc.

# REGULATORY GUIDANCE

# THREE PRIMARY REQUIREMENTS

## FFIEC GUIDANCE – EFFECTIVE JANUARY 1, 2012

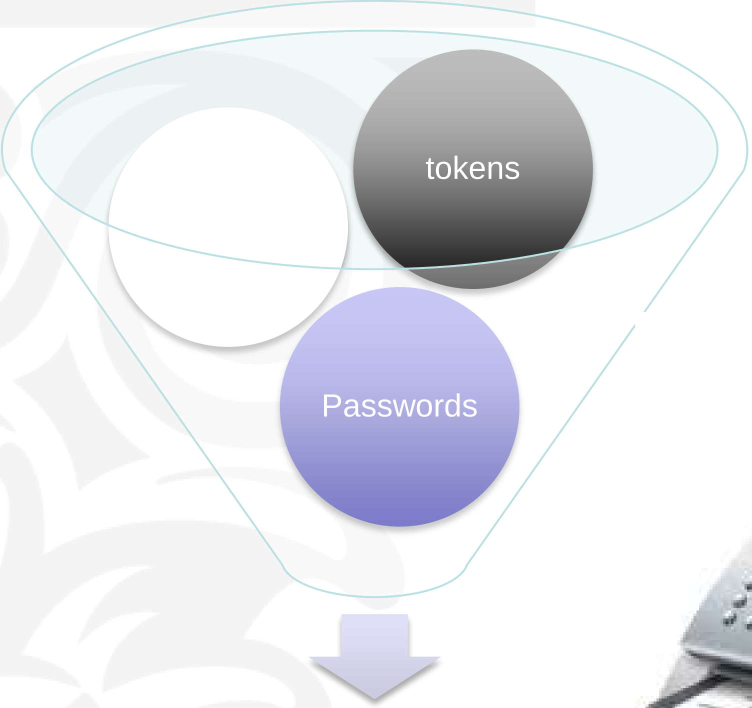


Risk Assessments

Layered Security

Education

# OUT-OF-BAND


tokens

Passwords

Internet

# CYBERSECURITY

# FFIEC GUIDANCE

## FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

# Framework for Improving Critical Infrastructure Cybersecurity

## Version 1.0

## February 12, 2014

# CYBERSECURITY

**The process for managing cyber threats and vulnerabilities and for protecting information and information systems by identifying, defending against, responding to, and recovering from attacks.**

# CYBER RESILIENCE IS CRUCIAL

- **If cyber resilience is not properly managed, a financial institution’s recovery from a cyber related incident may be unnecessarily delayed, lead to financial and legal repercussions, or preclude an institution from recovering at all.**

- **This is why it is important to include a cyber event in business continuity training and testing, both with employees and an institution’s third-party vendors.**

# CYBERSECURITY FRAMEWORK

**The Framework Core consists of five concurrent & continuous functions:**

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

# SR 15-9
# FFIEC CYBERSECURITY ASSESSMENT TOOL

**Overview for Chief Executive Officers and Boards of Directors**

**In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council(FFIEC) developed the Cybersecurity Assessment Tool (Assessment), on behalf of its members, to help institutions identify their risks and determine their cybersecurity preparedness. *The Assessment provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness over time.* The Assessment incorporates cybersecurity-related principles from the *FFIEC Information Technology (IT) Examination Handbook* and regulatory guidance, and concepts from other industry standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework.**

# BENEFITS TO THE INSTITUTION

**For institutions using the Assessment, management will be able to enhance their oversight and management of the institution’s cybersecurity by doing the following:**

- **Identifying factors contributing to and determining the institution’s overall cyber risk.**
- **Assessing the institution’s cybersecurity preparedness.**
- **Evaluating whether the institution’s cybersecurity preparedness is aligned with its risks.**
- **Determining risk management practices and controls that are needed or need enhancement and actions to be taken to achieve the desired state.**
- **Informing risk management strategies.**

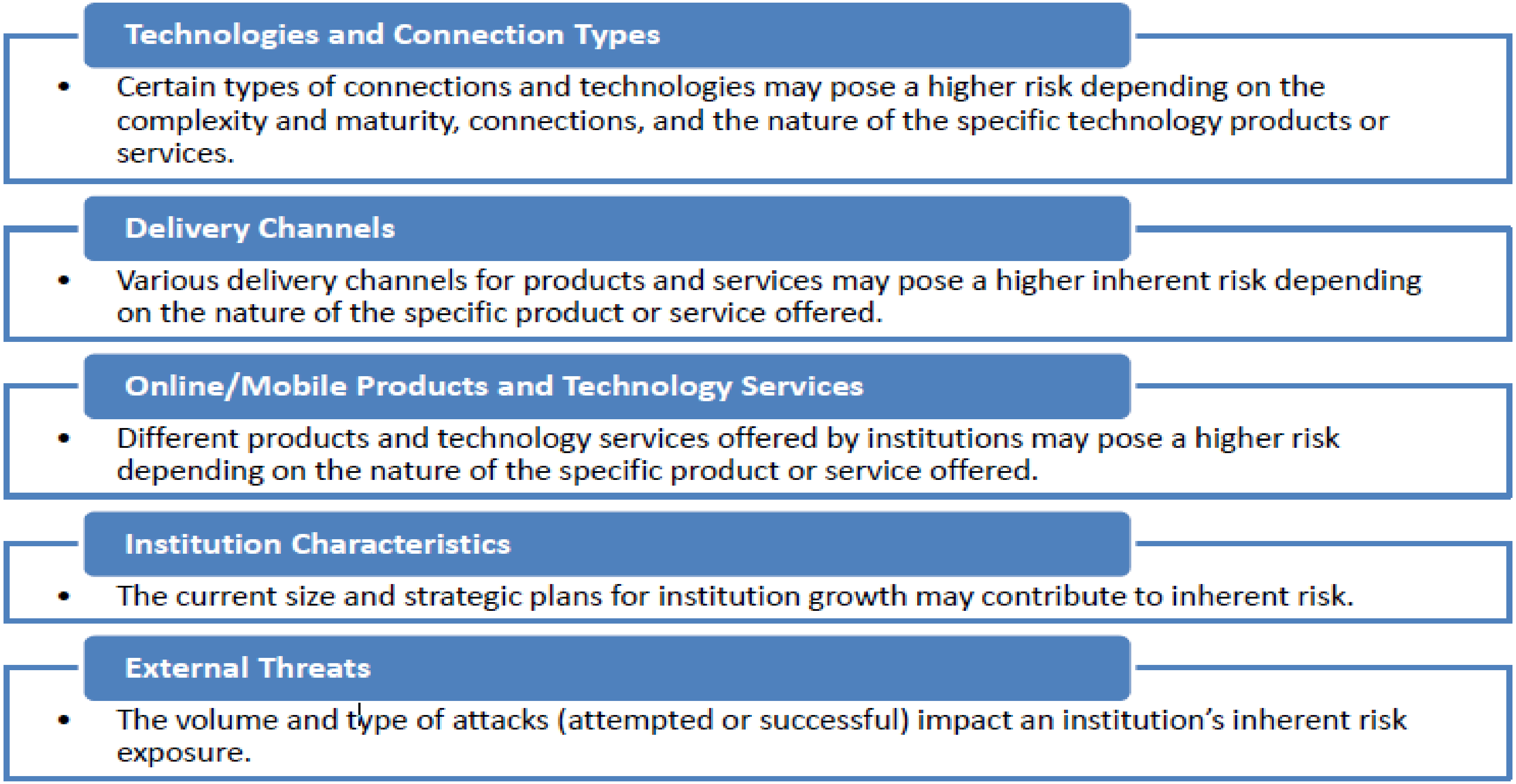
# ASSESSMENT’S PARTS AND PROCESS

**The Assessment consists of two parts:**

1. **Inherent Risk Profile**
2. **Cybersecurity Maturity**

**Upon completion of both parts, management can evaluate whether the institution’s inherent risk and preparedness are aligned.**

# INHERENT RISK PROFILE –RISK CATEGORIES



**Technologies and Connection Types**

- Certain types of connections and technologies may pose a higher risk depending on the complexity and maturity, connections, and the nature of the specific technology products or services.

**Delivery Channels**

- Various delivery channels for products and services may pose a higher inherent risk depending on the nature of the specific product or service offered.

**Online/Mobile Products and Technology Services**

- Different products and technology services offered by institutions may pose a higher risk depending on the nature of the specific product or service offered.

**Institution Characteristics**

- The current size and strategic plans for institution growth may contribute to inherent risk.

**External Threats**

- The volume and type of attacks (attempted or successful) impact an institution's inherent risk exposure.

# INHERENT RISK PROFILE –RISK LEVELS

### Least Inherent Risk

- An institution with a Least Inherent Risk Profile generally has very limited use of technology, few computers, applications, systems, and no connections. The variety of products and services are limited.

### Minimal Inherent Risk

- An institution with a Minimal Inherent Risk Profile generally has limited complexity in terms of the technology it uses. It offers a limited variety of less risky products and services.

### Moderate Inherent Risk

- An institution with a Moderate Inherent Risk Profile generally uses technology that may be complex in terms of volume and sophistication.

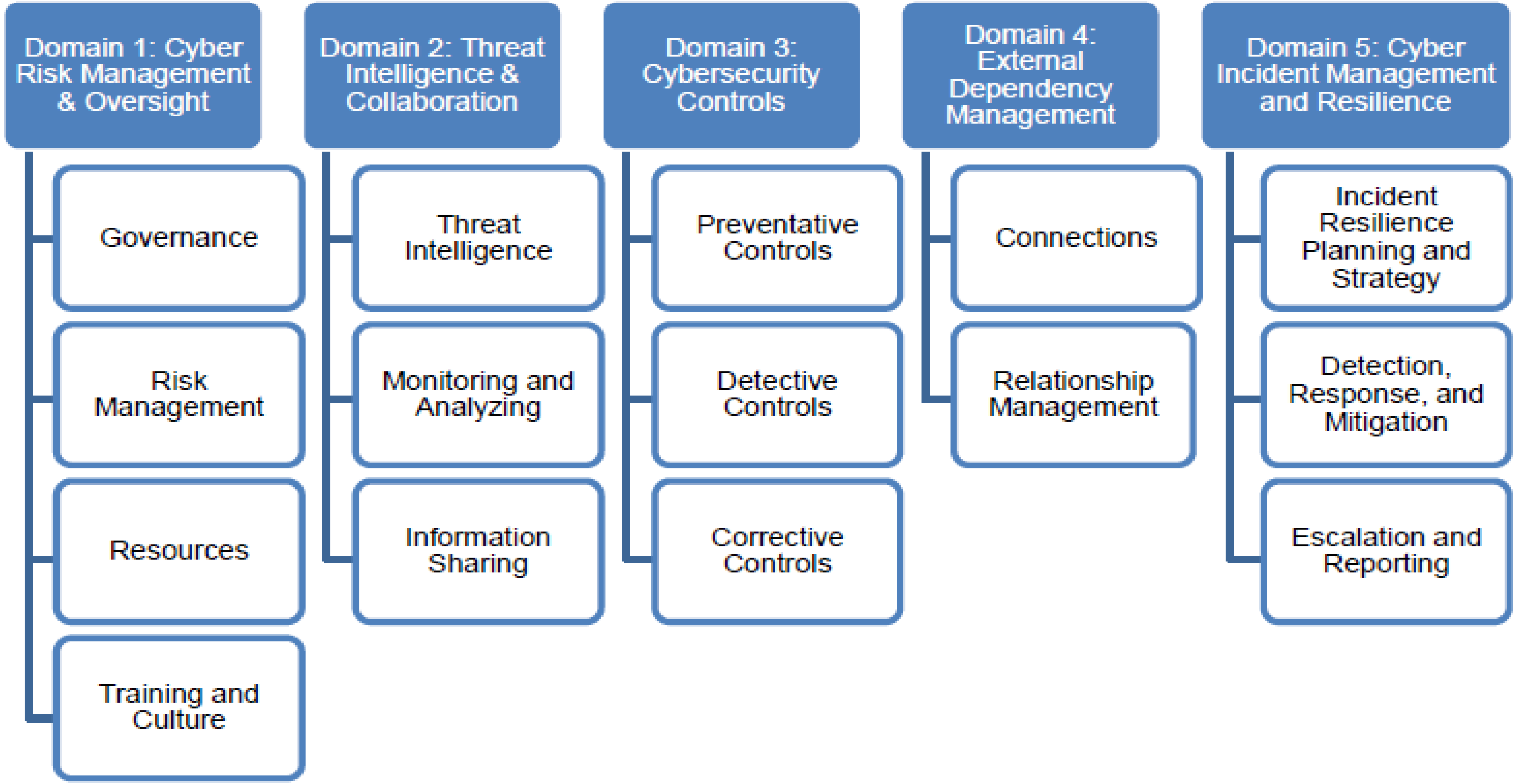
### Significant Inherent Risk

- An institution with a Significant Inherent Risk Profile generally uses complex technology in terms of scope and sophistication. The institution offers high-risk products and services that may include emerging technologies.

### Most Inherent Risk

- An institution with a Most Inherent Risk Profile uses extremely complex technologies to deliver myriad products and services. Many of the products and services are at the highest level of risk, including those offered to other institutions. New and emerging technologies are utilized across multiple delivery channels.

# FIVE DOMAINS & ASSESSMENT FACTORS



Domain 1: Cyber Risk Management & Oversight

- Governance
- Risk Management
- Resources
- Training and Culture

Domain 2: Threat Intelligence & Collaboration

- Threat Intelligence
- Monitoring and Analyzing
- Information Sharing

Domain 3: Cybersecurity Controls

- Preventative Controls
- Detective Controls
- Corrective Controls

Domain 4: External Dependency Management

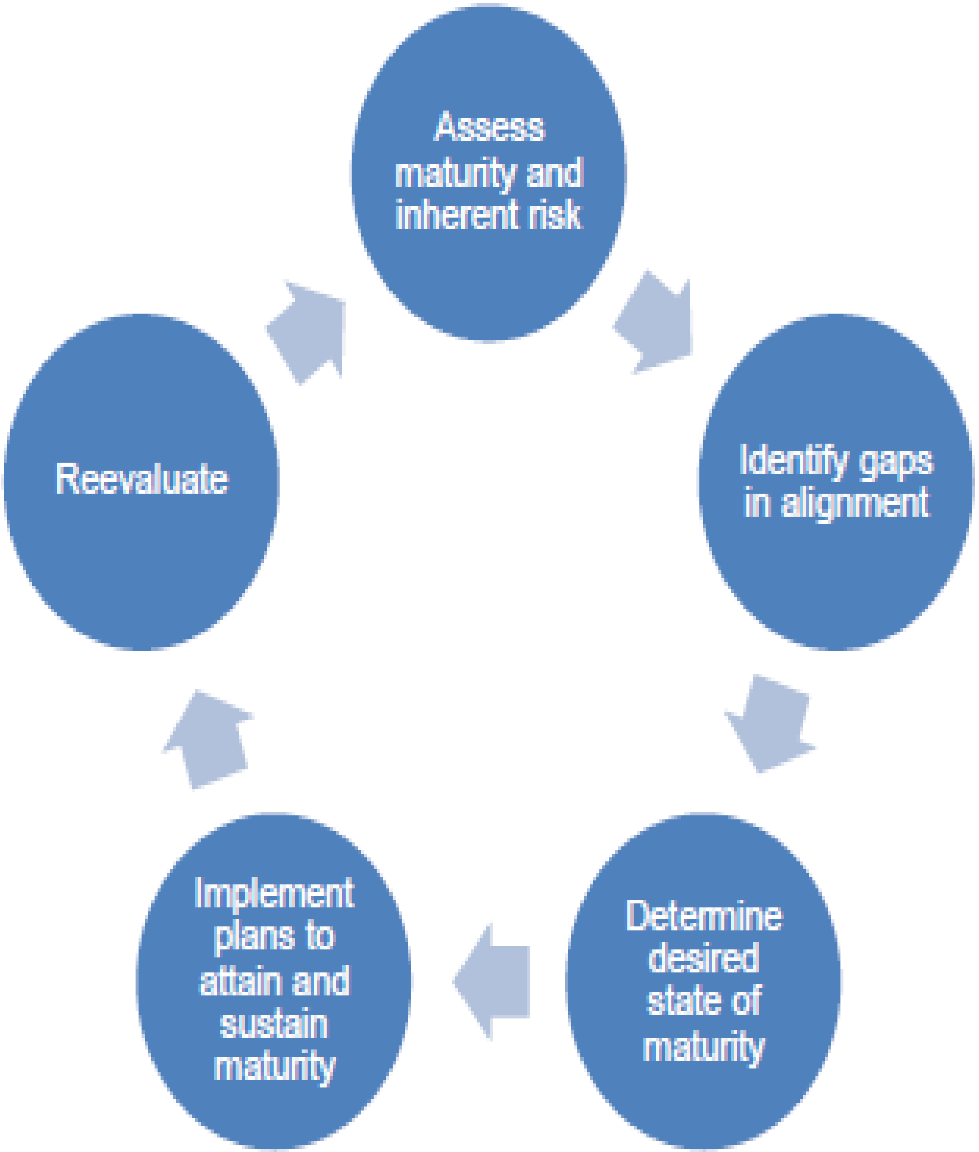
- Connections
- Relationship Management

Domain 5: Cyber Incident Management and Resilience

- Incident Resilience Planning and Strategy
- Detection, Response, and Mitigation
- Escalation and Reporting

# STEPS

1. **Complete Part One: Inherent Risk Profile**
2. **Complete Part Two: Cybersecurity Maturity Assessment**
3. **Determine appropriate target maturity level**
4. **Identify any gaps between current and desired states**
5. **Develop implementation plans based on identified gaps**

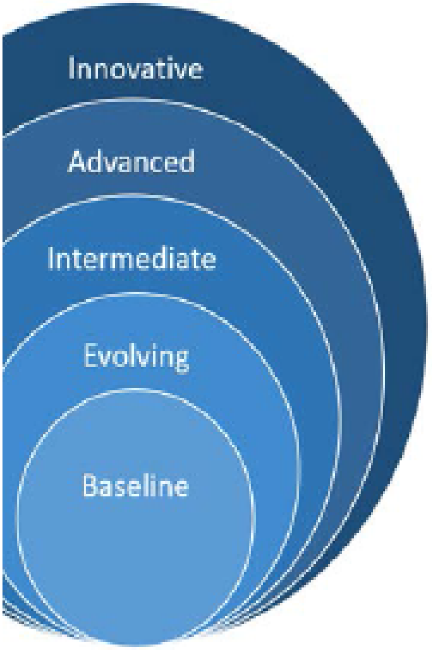

Assess maturity and inherent risk
Identify gaps in alignment
Determine desired state of maturity
Implement plans to attain and sustain maturity
Reevaluate

# CYBERSECURITY MATURITY

- **How effective are the institution’s risk management activities and controls identified in the Assessment?**
- **Are there more efficient or effective means for attaining or improving the institution’s risk management and controls?**
- **What third parties does the institution rely on to support critical activities?**
- **What is the process to oversee third parties and understand their inherent risks and cybersecurity maturity?**
- **How does management validate the type and volume of attacks?**
- **Is the institution sharing threat information with peers, law enforcement, and critical third parties through information-sharing procedures?**

# Maturity Assessment – Maturity Levels

| | |
|---|---|
| **Baseline** | Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in guidance. It includes compliance-driven objectives. Management has reviewed and evaluated guidance. |
| **Evolving** | Evolving maturity is characterized by additional formality of documented procedures and policies which are not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond protection of customer information to incorporate information assets and systems. |
| **Intermediate** | Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk-management practices and analysis are integrated into business strategies. |
| **Advanced** | Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across the lines of business. Risk management processes are automated and include continuous process improvement. Accountability for risk decisions by front-line businesses is formally assigned. |
| **Innovative** | Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry. This may entail developing new controls, new tools, or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses. |



# SIX-STEP CYBER THREAT INTELLIGENCE PROCESS FOR FINANCIAL INSTITUTIONS

1. **Know your SPECIFIC threats and vulnerabilities.**
2. ***Establish outside sources of threat intelligence for your threats.***
3. **Actively and continuously adjust your security controls and monitoring as appropriate to mitigate those threats.**
4. **Have detailed incident plans for responses to the threats, and update these plans periodically as appropriate.**
5. **Actively adjust your intelligence-gathering goals to address the changes in your threats and risks.**
6. **Additionally conduct a cyber threat analysis as part of your overall risk management governance and compliance program.**

# THREAT INTELLIGENCE INFORMATION SOURCES

**Government and Institutional Resources**

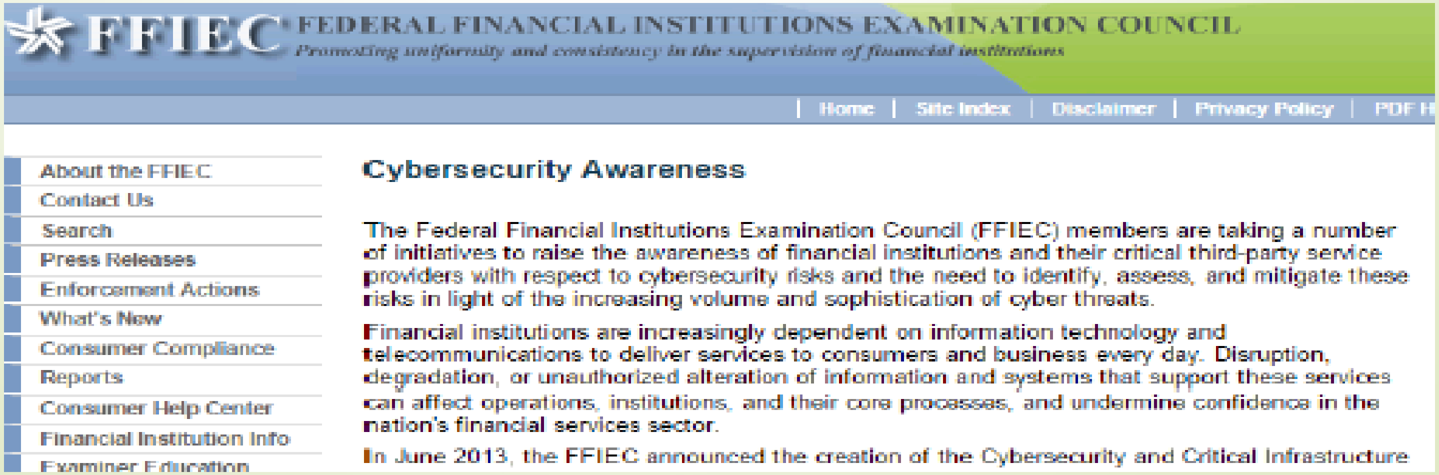
- Federal Bureau of Investigation (FBI)
  - Infragard
- United States Secret Service (USSS)
  - Electronic Crimes Task Force
- Department of Homeland Security (DHS)
  - United States Computer Emergency Readiness Team (US-CERT)
- National Cybersecurity and Communications Integration Center (NCCIC)
- Financial Crimes Enforcement Network (FinCEN)
- Common Vulnerability Enumeration Database (CVE)
- National Vulnerability Database

**Sector, Industry and Technology-Focused Resources**

- Financial Services-Information Sharing and Analysis Center (FS-ISAC)
- Competitors, partners, and financial industry associations
- Industry news sites, e.g. krebsonsecurity.com, bankinfosecurity.com
- Information security sector sites, e.g. Internet Storm Center, Open Threat Exchange (OTX), ATLAS
- Managed security service providers (MSSPs) – blogs and feeds

# FFIEC Cyber Security

- Main Site: https://www.ffiec.gov/cybersecurity.htm
- Board/Senior Management Video: http://youtu.be/t1ZgWKjynXI
- Observations: https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf


FFIEC
FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions
| Home | Site Index | Disclaimer | Privacy Policy | PDF H
About the FFIEC
Contact Us
Search
Press Releases
Enforcement Actions
What's New
Consumer Compliance
Reports
Consumer Help Center
Financial Institution Info
Examiner Education

## Cybersecurity Awareness

The Federal Financial Institutions Examination Council (FFIEC) members are taking a number of initiatives to raise the awareness of financial institutions and their critical third-party service providers with respect to cybersecurity risks and the need to identify, assess, and mitigate these risks in light of the increasing volume and sophistication of cyber threats.

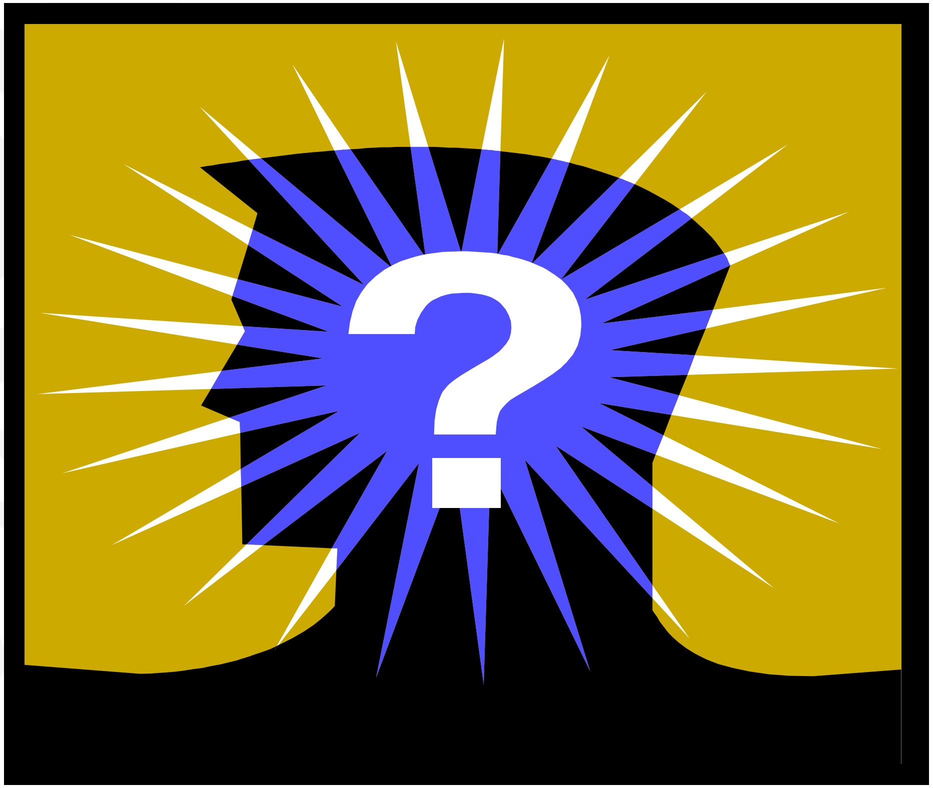
Financial institutions are increasingly dependent on information technology and telecommunications to deliver services to consumers and business every day. Disruption, degradation, or unauthorized alteration of information and systems that support these services can affect operations, institutions, and their core processes, and undermine confidence in the nation's financial services sector.

In June 2013, the FFIEC announced the creation of the Cybersecurity and Critical Infrastructure

# SUMMARY

- Understand your inherent risk relating to cybersecurity
- Monitor and manage sufficient awareness of continuing and emerging threats and vulnerabilities
- Ensure you have established a dynamic control environment
- Understand the responsibilities of third parties and manage them effectively
- Test your BC and DR plans against cybersecurity scenarios
- Involve the Board of Director and Senior Management to provide oversight

# QUESTIONS



# FOR MORE INFORMATION

**FBI Alert: Fraudulent ACH Transfers**

**http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm**

**FDIC Special Alert: Fraudulent Electronic Funds Transfers**

**http://www.fdic.gov/news/news/SpecialAlert/2009/sa09147.html**

**FDIC Special Alert SA-185-2009 Fraudulent Funds Transfer Schemes**

**http://www.fdic.gov/news/news/SpecialAlert/2009/sa09185.html**

**NACHA Bulletin: Corporate Account Takeovers**

**http://www.nacha.org/docs/NACHA%20Operations%20Bulletin%20-%20Corporate%20Account%20Takeover%20-%20December%202,%202009.pdf**

# FOR MORE INFORMATION

- FFIEC IT Handbooks
  http://ithandbook.ffiec.gov
- FFIEC Cybersecurity Awareness Web Site
  http://ffiec.gov/cybersecurity.htm
- Financial Stability Oversight Council 2015 Annual Report
  http://www.treasury.gov/initiatives/fsoc/studies-reports/Pages/2015-Annual-Report.aspx
- The FDIC's "Cyber Challenge: A Community Bank Cyber Exercise"
  http://www.fdic.gov/regulations/resources/director/technical/cyber/cyber/htm
- Financial Services-Information Sharing and Analysis Center (FS-ISAC) www.fsisac.com/
- United States Computer Emergency Readiness Team (US-CERT)
  www.us-cert.gov/
- InfraGard
  www.infragard.org/
- U.S. Secret Service Electronic Crimes Task Force www.secretservice.gov/ectf.shtml
- The Top Cyber Threat Intelligence Feeds
  www.thecyberthreat.com/cyber-threat-intelligence-feeds/

# REGULATORY GUIDANCE

- **SR 15-3: Strengthening the Resilience of Outsourced Technology Services**
- **SR 15-9: FFIEC Cybersecurity Assessment Tool**
- **SR 12-14: Revised Guidance on Supervision of Technology Service Providers**
- **SR 11-9: Interagency Supplement to Authentication in an Internet Banking Environment**
- **SR 09-2: FFIEC Guidance Addressing Risk Management of Remote Deposit Capture**
- **SR 06-13: Q&A Related to Interagency Guidance on Authentication in an Internet Banking Environment**

# REGULATORY GUIDANCE CONTINUED

- **SR 05-23: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice**
- **SR 05-19: Interagency Guidance on Authentication in an Internet Banking Environment**
- **FFIEC Risk Management of Remote Deposit Capture**
- **FFIEC Information Security Booklet**
- **SR 01-15: Standards for Safeguarding Customer Information**
- **SR 01-11: Identity Theft and Pretext Calling—(attachment) Interagency Guidelines Establishing Standards for Safeguarding Customer Information**

# VENDOR RESOURCES & REFERENCES

- FFIEC
- IBM
- Trusteer
- REUTERS
- Bloomberg Business Week
- ThreatMetrix
- Akamai
- FBI
- Symantec
- Trustwave, Inc.
- NIST
- SurfWatch
- enews@bankinfosecurity.com