AAII Silicon Valley Chapter Meeting
September 14, 2019

- **FINANCIAL SERVICES CYBERSECURITY and THE CHANGING WORLD!**
- **Ed Machado, CRISC, CISM, Privacy Officer/Information Security Officer**
- edfmac_2000@yahoo.com
- **Mobile 408-390-1187**

Agenda

- Cyber Terminologies
- Anatomy of a Breach
- Financial Services Cyber Threat Word
- Malware and Viruses
- Computer and Internet Fraud Scams
- Social Engineering, Phishing and Smishing
- Personal Security Best Practices Review
- Questions and Answers

Cyber Terminologies

- **Hacker/Cyber Criminal**: Person who seeks to exploit people, computers or systems for their own gain.
- **Malicious Code**: Sometimes called **Malware,** this is code used to attack your computer to do something (steal personal info or corrupt other systems).
- **Ransomware – Malicious Code** with the intent purpose to encrypt files on a computer and request payment via Bitcoin or Cryptocurrency to release the code to unencrypt the files.
- **Viruses/Trojans: Malicious Code** with intent to corrupt or make systems inoperable.
- **Cryptocurrency**: is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency

Cyber Terminologies

- **Hacker/Cyber Criminal:** Person who seeks to exploit people, computers or systems for their own gain.
- **Malicious Code:** Sometimes called **Malware,** this is code used to attack your computer to do something (steal personal info or corrupt other systems).
- **Ransomware – Malicious Code** with the intent purpose to encrypt files on a computer and request payment via Bitcoin or Cryptocurrency to release the code to unencrypt the files.
- **Viruses/Trojans: Malicious Code** with intent to corrupt or make systems inoperable.
- **Cryptocurrency**: is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency

Cyber Terminologies

- **Bitcoin:** is a worldwide **cryptocurrency** and digital payment system called the first decentralized digital currency, since the system works without a central repository or single administrator. Bitcoin is accepted 100,000 merchants/vendors as a form of payment.
- **Vulnerability:** Programming errors in software for which a **Hacker** can take advantage of to infect a computer or systems with **Malicious Code.**
- **Social Engineering:** A **Hacker** uses some form of human interaction (social skills),email or website to obtain information about a person, organization or system.
- **Phishing**: This is a form of **Social Engineering** where a **Hacker** uses email or a website to solicit personal information by posing as a trustworthy organization**.**
- **Vishing:** This is a form of **Social Engineering** to obtain information using the phone.

Anatomy of a Data Breach

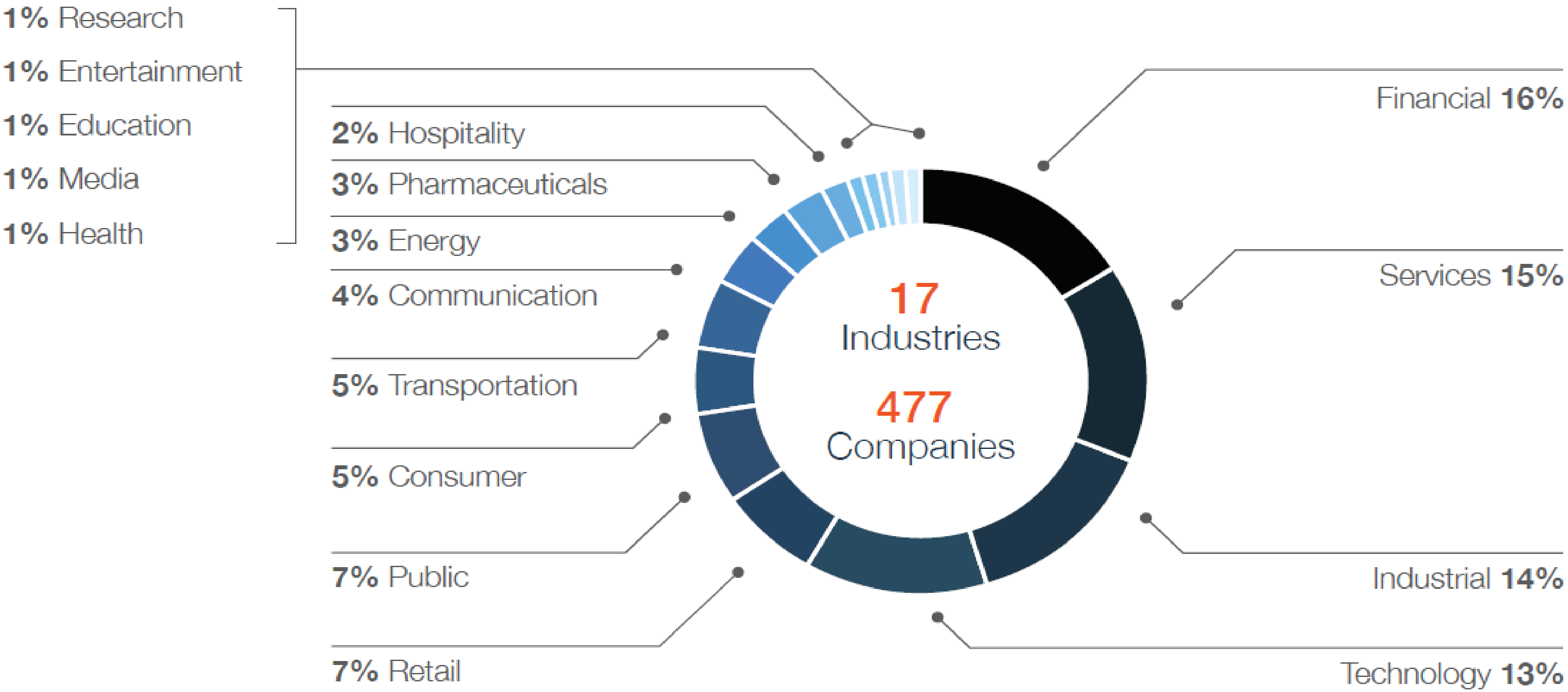
- Phishing – Credentials Compromised by clicking and input of data!
- Poor Security Practices– Known Exploit or Vulnerabilities in Windows– Federal Express/City Of Atlanta–WannaCry Ransomeware– North Korea?
- 3rd Party Providers aka Target Compromise

2018 Cost of a Data Breach Study: Global Overview

- U.S. based breaches are the most expensive globally, costing on average $7.91M with the average global notification cost totaling in excess of $700K or more.
- 48% of all breaches were caused by malicious or criminal attacks.
- Incident response teams and the extensive use of encryption reduce costs.
- Third party involvement in a breach and extensive cloud migration at the time of the breach increases the cost.
- The loss of customer trust has serious financial consequences. (reputation risk)
- Mean-time-to-identify (MTTI) a breach is 197 days, and the mean-time-to-contain (MTTC) is 69 days.
- Reported Global Business Email Compromises or CEO Imposter Fraud losses reached $12B globally (FBI)

Figure 38. Distribution of the sample by industry

Sample size (n) = 477



Today’s Threat Landscape

Targets

68% of financial institutions took months or longer to discover breaches

58% of breach victims were smaller institutions

80% of financial institutions replaced or augmented their existing AV solutions

Threat actors

73% of breaches are perpetrated by outsiders

60% of breaches are conducted by organized crime

92% of breaches originated through email

Tools

21% decrease in executables in favor of evasive, fileless techniques

87% of compromises took minutes to execute

37% of malware hashes only appeared once

The Bad Guys Are Getting More Sophisticated

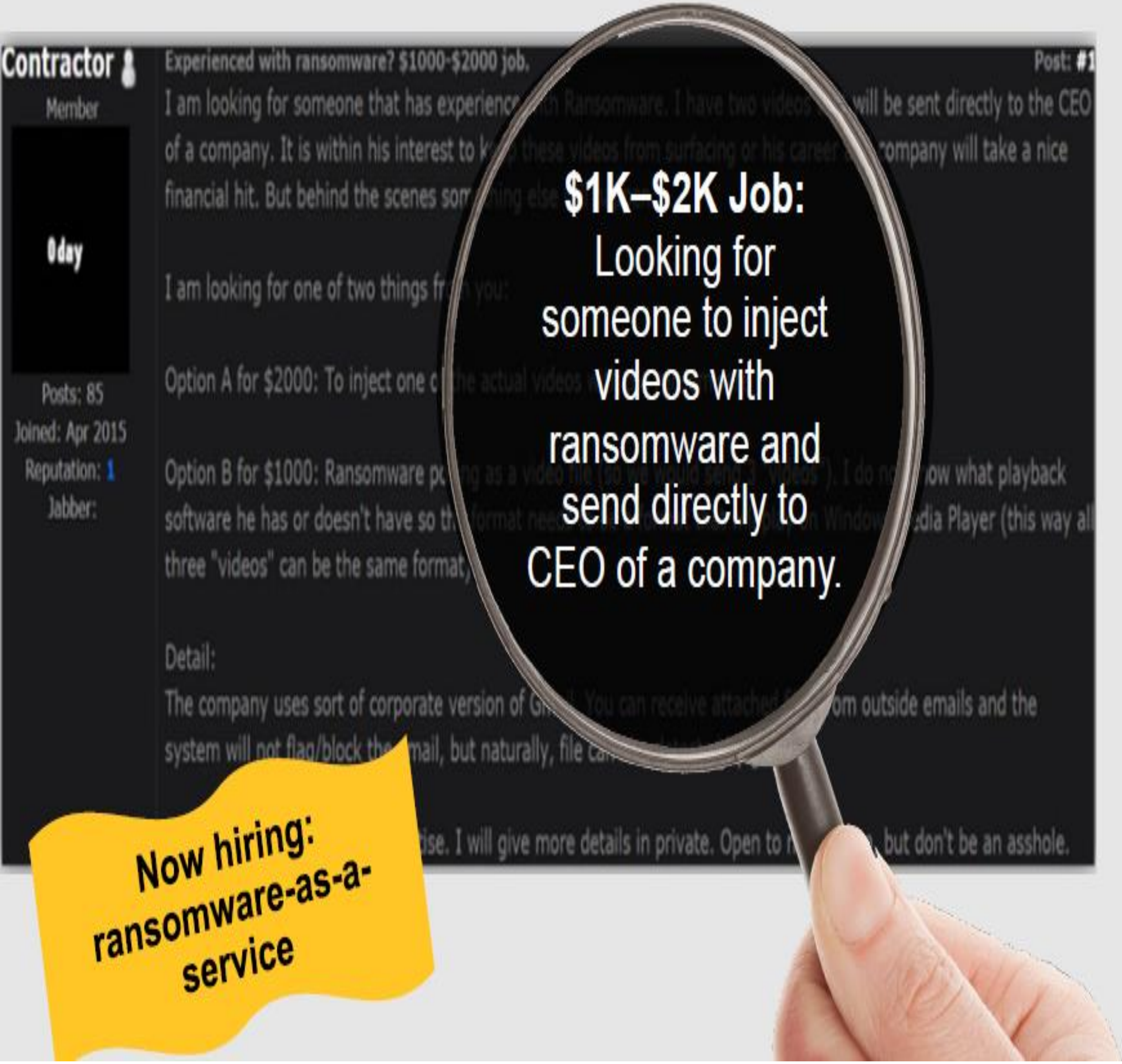
Dynamically modifying malware based on the environment and defenses encountered

Crowdsourcing in the “deep” and “dark” web

Point-and-click malware

Flooding threat intelligence with false positives

Hackers Buy and Sell Services on the Dark Web



Contractor
Member
0day
Posts: 85
Joined: Apr 2015
Reputation: 1
Jabber:

Experienced with ransomware? $1000-$2000 job. Post: #1

I am looking for someone that has experience with Ransomware. I have two videos will be sent directly to the CEO
of a company. It is within his interest to k these videos from surfacing or his career company will take a nice
financial hit. But behind the scenes som

I am looking for one of two things fr you:

Option A for $2000: To inject one c

Option B for $1000: Ransomware po ow what playback
software he has or doesn't have so th dia Player (this way all
three "videos" can be the same format,

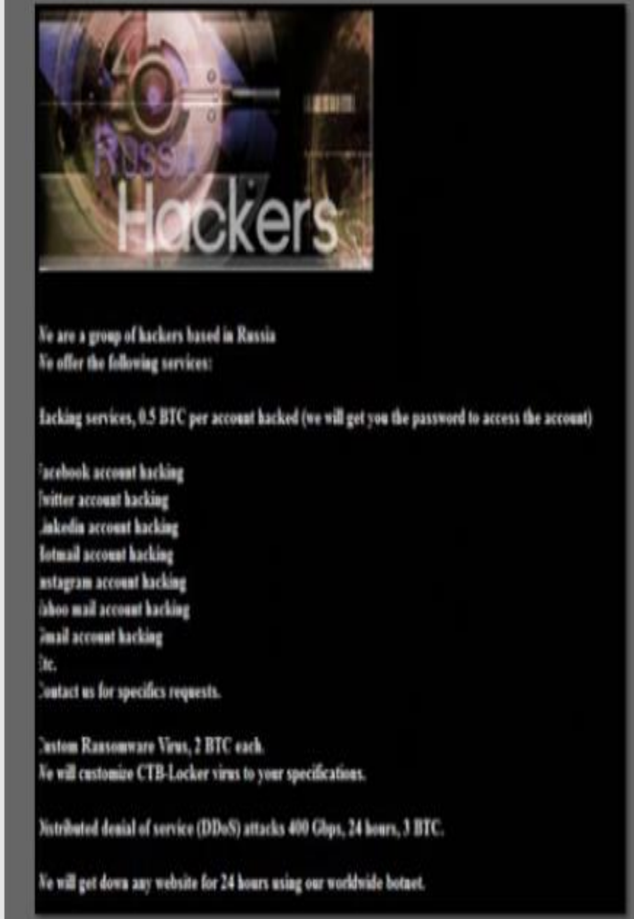
Detail:
The company uses sort of corporate version of G om outside emails and the
system will not flag/block th mail, but naturally, file ca

ise. I will give more details in private. Open to , but don't be an asshole.

$1K–$2K Job:
Looking for someone to inject videos with ransomware and send directly to CEO of a company.

Now hiring: ransomware-as-a-service

Hackers for hire



Ve are a group of hackers based in Russia
Ve offer the following services:

Iacking services, 0.5 BTC per account hacked (we will get you the password to access the account)

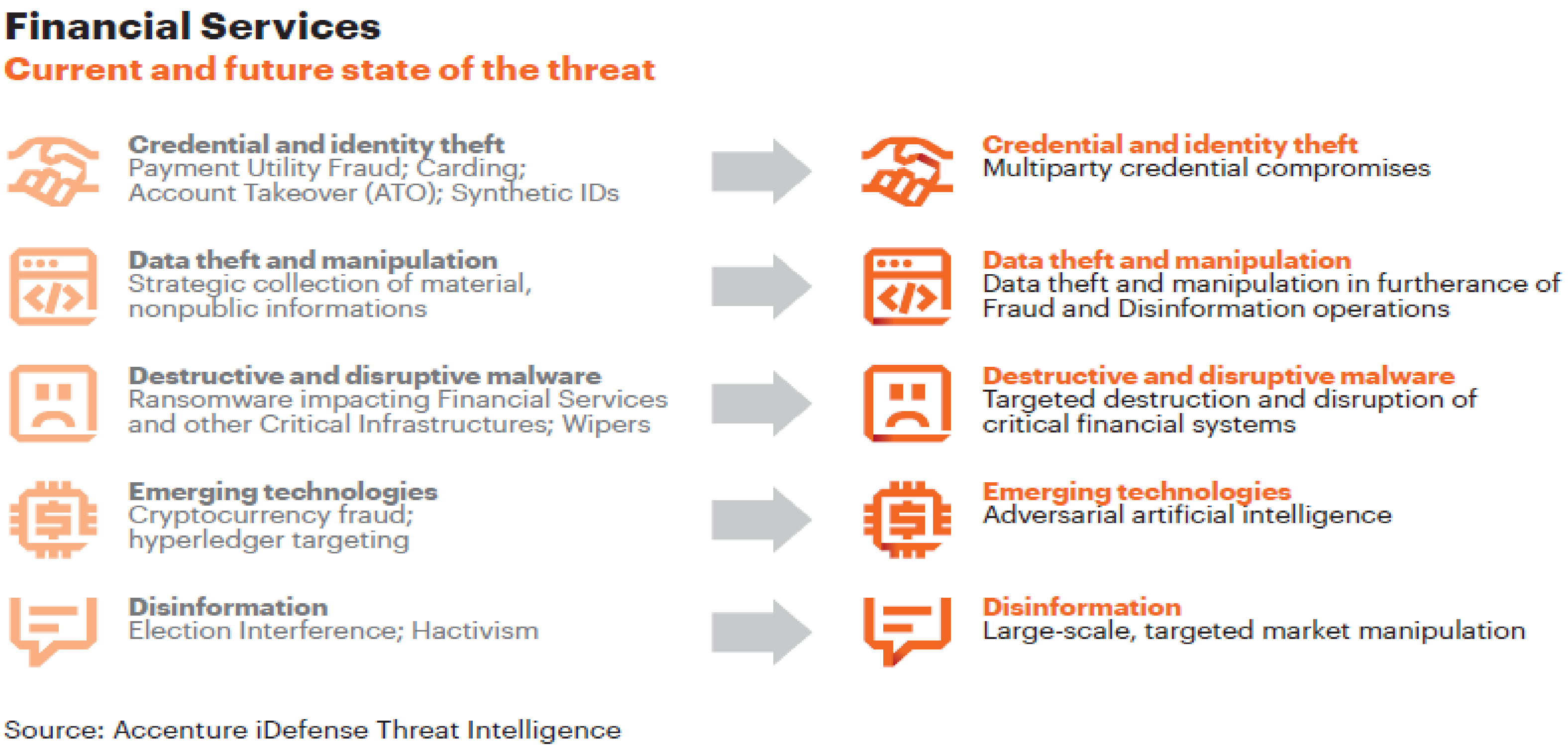
'acebook account hacking
'witter account hacking
.inkedin account hacking
Iotmail account hacking
nstagram account hacking
'ahoo mail account hacking
Gmail account hacking
Etc.
Contact us for specifics requests.

Custom Ransomware Virus, 2 BTC each.
Ve will customize CTB-Locker virus to your specifications.

Distributed denial of service (DDoS) attacks 400 Gbps, 24 hours, 3 BTC.

Ve will get down any website for 24 hours using our worldwide botnet.

Future Financial Services Key Threats



Financial Services

Current and future state of the threat

Credential and identity theft
Payment Utility Fraud; Carding;
Account Takeover (ATO); Synthetic IDs

→ **Credential and identity theft**
Multiparty credential compromises

Data theft and manipulation
Strategic collection of material, nonpublic informations

→ **Data theft and manipulation**
Data theft and manipulation in furtherance of Fraud and Disinformation operations

Destructive and disruptive malware
Ransomware impacting Financial Services and other Critical Infrastructures; Wipers

→ **Destructive and disruptive malware**
Targeted destruction and disruption of critical financial systems

Emerging technologies
Cryptocurrency fraud;
hyperledger targeting

→ **Emerging technologies**
Adversarial artificial intelligence

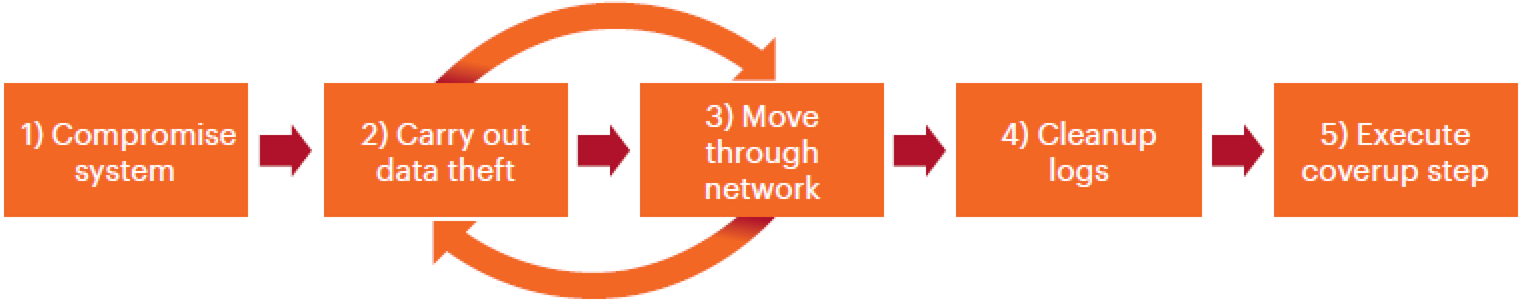
Disinformation
Election Interference; Hactivism

→ **Disinformation**
Large-scale, targeted market manipulation

Source: Accenture iDefense Threat Intelligence

Anatomy of a Breach or Data Theft Cover Up

Anatomy of the coverup



1) Compromise system

2) Carry out data theft

3) Move through network

4) Cleanup logs

5) Execute coverup step

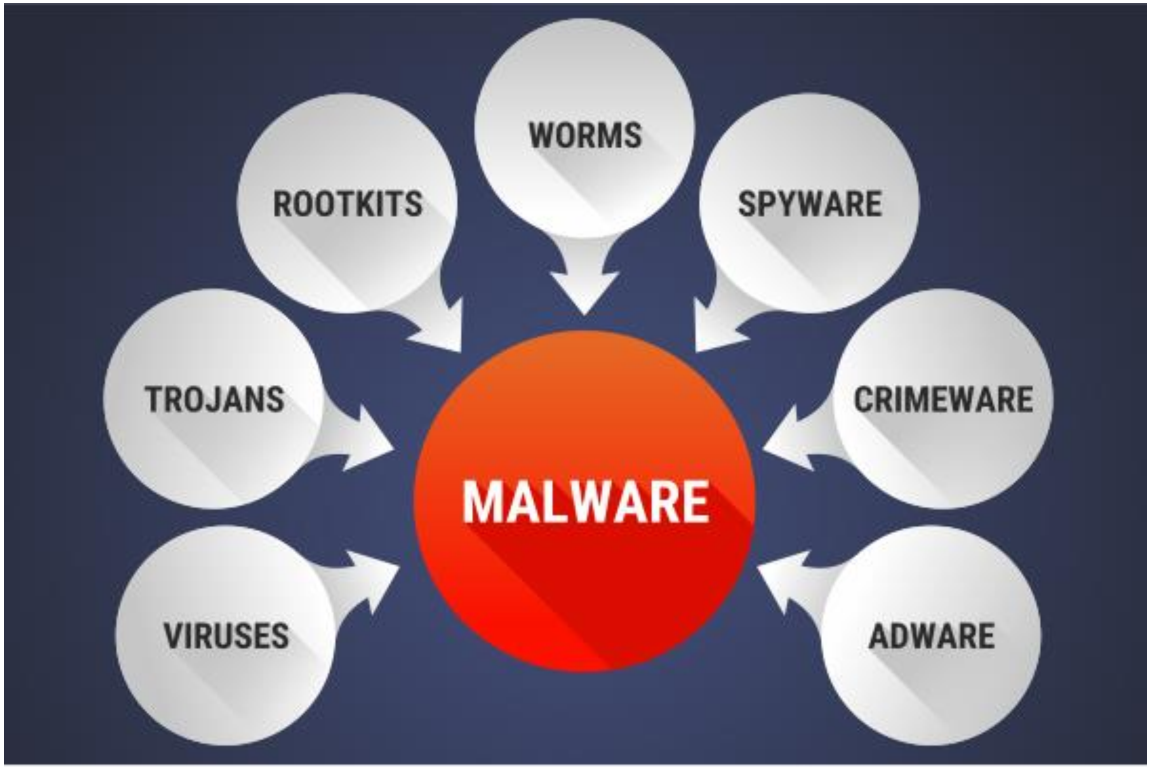
Source: Accenture iDefense Threat Intelligence

Malware and Viruses

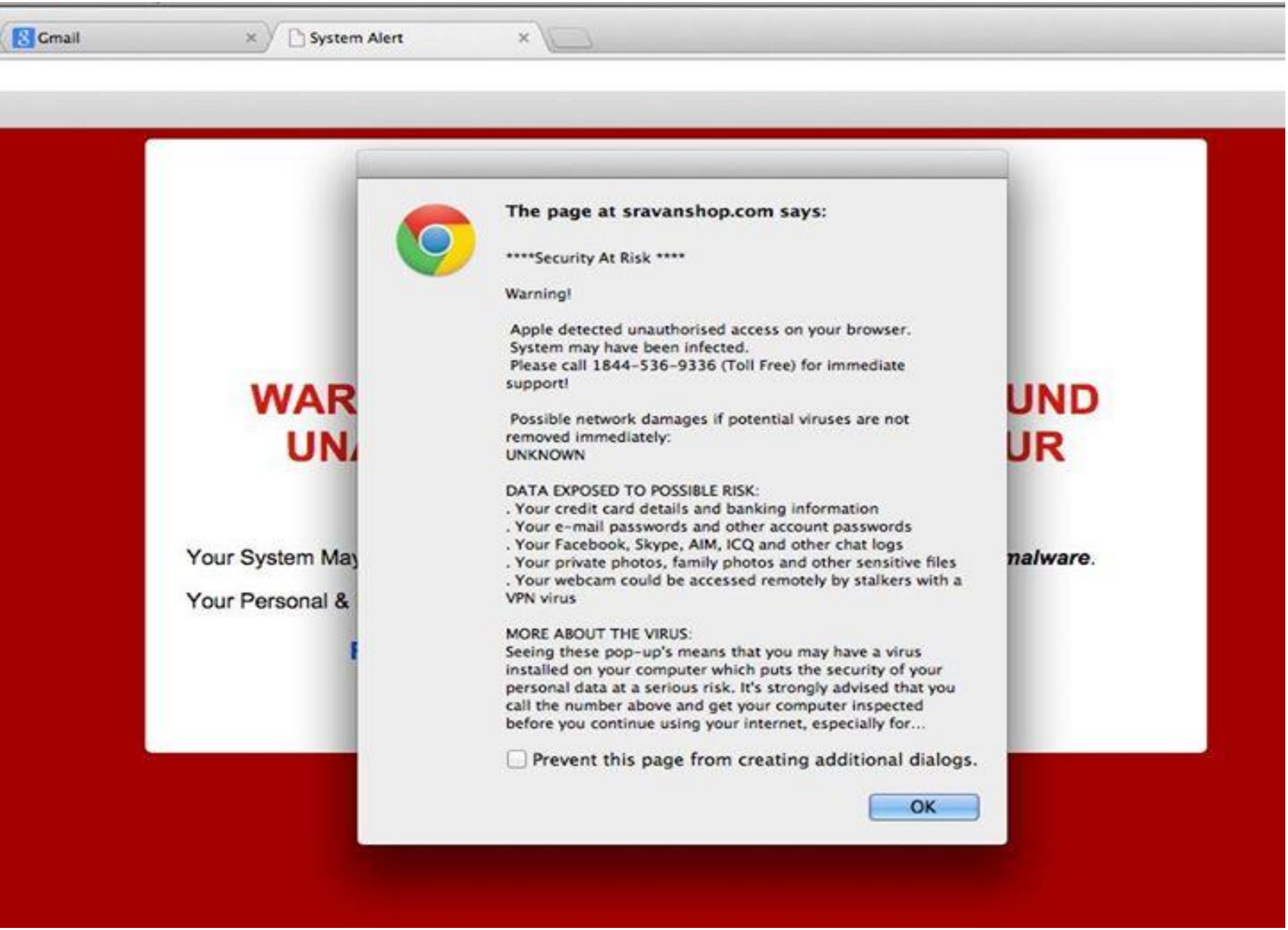
- Subscribe to a reputable Anti-Virus software provider and keep it up to date!
- Keep Operating System software up to date!
- Visit Reputable Websites- don’t click on Ads!
- Think Before You Click (Website, Email, Links)!

“Malware” – On PCs & Devices

Programs that spy on online sessions, harvest info, corrupt files, sell you things, and more.



Malware sometimes requires professional assistance to remove.



The page at sravanshop.com says:

****Security At Risk ****

Warning!

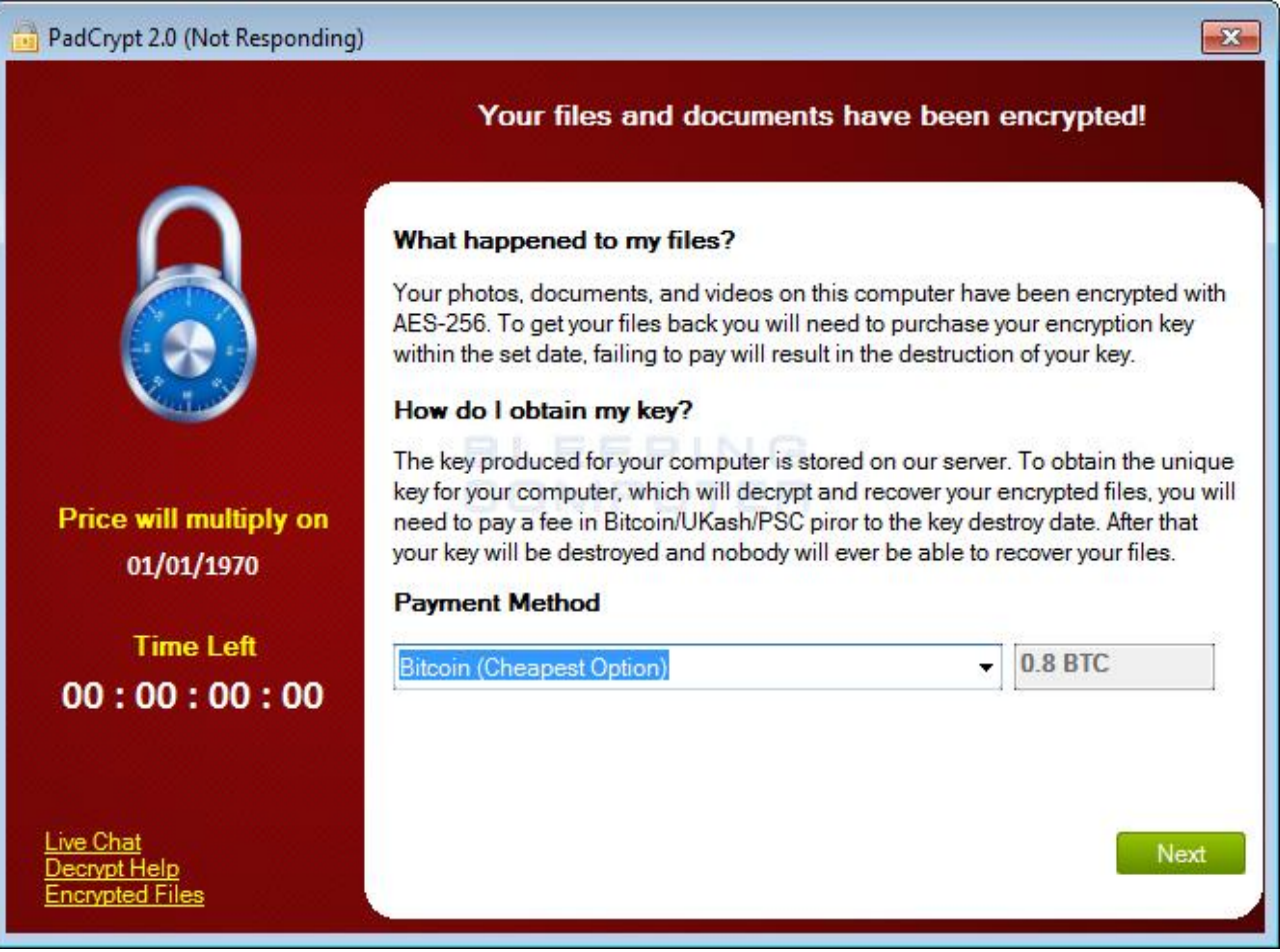
Apple detected unauthorised access on your browser.
System may have been infected.
Please call 1844-536-9336 (Toll Free) for immediate support!

Possible network damages if potential viruses are not removed immediately:
UNKNOWN

DATA EXPOSED TO POSSIBLE RISK:
. Your credit card details and banking information
. Your e-mail passwords and other account passwords
. Your Facebook, Skype, AIM, ICQ and other chat logs
. Your private photos, family photos and other sensitive files
. Your webcam could be accessed remotely by stalkers with a VPN virus

MORE ABOUT THE VIRUS:
Seeing these pop-up's means that you may have a virus installed on your computer which puts the security of your personal data at a serious risk. It's strongly advised that you call the number above and get your computer inspected before you continue using your internet, especially for...

□ Prevent this page from creating additional dialogs.



PadCrypt 2.0 (Not Responding)

Your files and documents have been encrypted!

What happened to my files?

Your photos, documents, and videos on this computer have been encrypted with AES-256. To get your files back you will need to purchase your encryption key within the set date, failing to pay will result in the destruction of your key.

How do I obtain my key?

The key produced for your computer is stored on our server. To obtain the unique key for your computer, which will decrypt and recover your encrypted files, you will need to pay a fee in Bitcoin/UKash/PSC piror to the key destroy date. After that your key will be destroyed and nobody will ever be able to recover your files.

Payment Method

Bitcoin (Cheapest Option) 0.8 BTC

Price will multiply on
01/01/1970

Time Left
00 : 00 : 00 : 00

Scams, Authorized Use & Fraud

<u>Scams</u>

- Computer – card number to fix PC
- Gift Cards for Payment of Services – IRS, bail,
  - –Apple, CVS, Walgreens, etc.

<u>Authorized Use</u>

- Giving your card to someone
- Free Trial Offers – free is not free

<u>Fraud</u>

- Did not give your card or card info to someone

How to Prevent/Reduce Exposure

Tips

- Do not provide card information unless you initiate
- Current Contact Information
- Travel Advisories
- Monitor your account

Tools?

- Temporary card blocks – Online & Mobile
- Real time Alerts (Visa Purchase Alerts, coming soon 2 way fraud alerts)

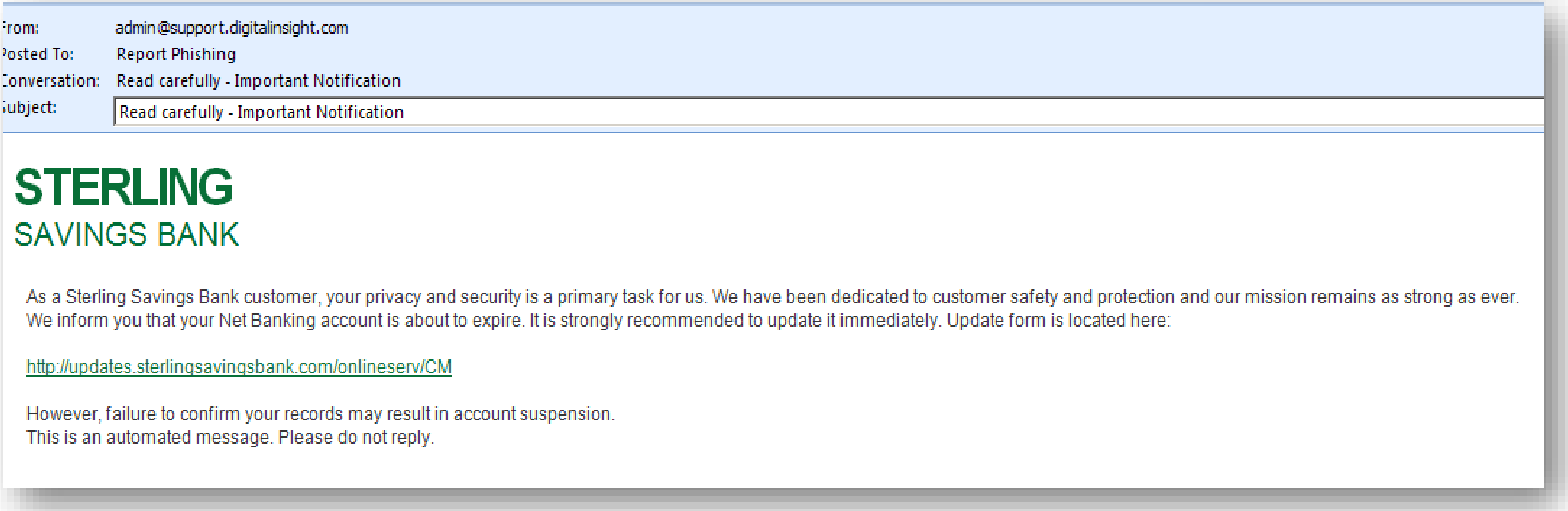
Online Threats

- Phishing
- Smishing
- Social
- Public Wi-Fi

You have just won $ 100 gift voucher. If you want it pls click here..
Click Me

“Phishing” - Email

An email attempt to acquire information by masquerading as a trustworthy entity.



rom: admin@support.digitalinsight.com
osted To: Report Phishing
onversation: Read carefully - Important Notification
ubject: Read carefully - Important Notification

STERLING
SAVINGS BANK

As a Sterling Savings Bank customer, your privacy and security is a primary task for us. We have been dedicated to customer safety and protection and our mission remains as strong as ever. We inform you that your Net Banking account is about to expire. It is strongly recommended to update it immediately. Update form is located here:

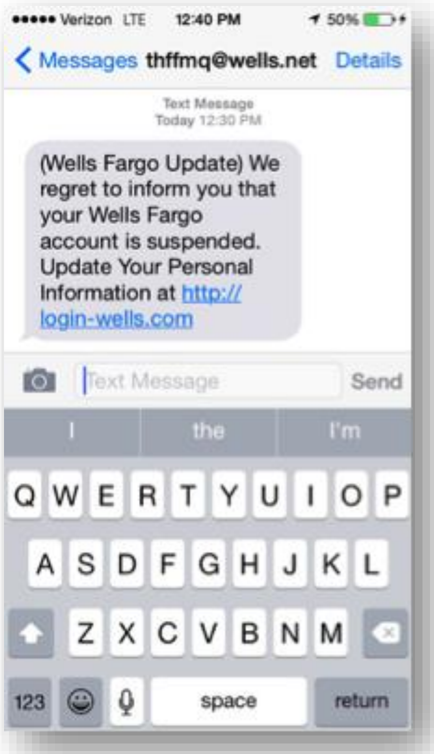
http://updates.sterlingsavingsbank.com/onlineserv/CM

However, failure to confirm your records may result in account suspension.
This is an automated message. Please do not reply.

Clicking the link may allow a backdoor into your PC.

"Smishing" - Text Message

A "Smishing" text message is designed to trick you by masquerading as a trustworthy entity.



Messages thffmq@wells.net Details

Text Message
Today 12:30 PM

(Wells Fargo Update) We regret to inform you that your Wells Fargo account is suspended. Update Your Personal Information at http://login-wells.com

https://www.youtube.com/watch?v=-iNKBzD4aF8

Selecting the link may allow a backdoor into your device.

"Social Engineering"

Everyone is vulnerable

Phone Calls:

Tech Support – "Fix" your PC – they request Credit Card

ent

IRS Agent – "Pay now" - to keep authorities away
Police – "Your Grandson is in trouble" – he asks for bail $
Ransom – "Your Grandson is captive" – they ask for ransom $
Your Bank/CU – "Account is Compromised" – they ask for your

Facebook/Instagram/Twitter:

They assume your Identity – Make your accounts "Private"
On Vacation? – Don't tell the world when/where you are going
Instant Msg. (Yahoo/Facebook) – Don't click links, even from
friends

Pop-Ups & Ads have viruses – Don't click them as a practice
Online Quizzes – They harvest your info – Don't take them

Public Wi-Fi

- Easy for fraudsters to put up fake “Wi-Fi” hotspots – Pineapple Device (purchase on the web) – “Man in the Middle Attacks” Do Not login into your Email account on unsecure Public Wi-Fi
- Do Not perform Online Banking on unsecure Public Wi-Fi
- Do Not perform Shopping (Amazon) on unsecure Public Wi-Fi
- Secure Your home “Wi-Fi” network (password with WPA or WPA2). WPA/WPA2 is “Wi-Fi Encryption” known as “Wi-Fi Protected Access” and uses a password/passphrase
- Always turn-off “Wi-Fi” when not in-use
- Always turn off “Bluetooth” when not in use

Personal Privacy Protection

- Do not share all information on Social Media (vacations, workplace, title, family, etc.)
- Use Multi-Factor Authentication as available (Facebook, Yahoo, Gmail, Twitter, Online Banking)
- Do not use the same username and password for all sites (compromise one/compromise all)– “The Daisy Chain Affect”
- Use Complex Passwords– Not Easy to Guess
- Use “Enhanced Privacy” options

Review– Cyber Security Best Practices

- Stop, Think, Connect before you Click!
- Use the “Delete” key for unknown email
- Backup Your Files (iCloud, USB or other storage media)
- Update Your Software (Microsoft, Apple IOS, Android)
- Subscribe and keep Anti-Virus software current with auto update
- Consider using 2 Factor Authentication

Review- Cyber Security Best Practices

- Protect Your Identity- Think before you give it out or why it is needed (email or phone)
- Protect Your Passwords (Complex, Different for Accounts, Do Not Share)
- Avoid Using Public Wi-Fi for access to sensitive information (mail, online banking, shopping)
- Turn off Wi-Fi and Bluetooth when not actively being used

Cyber Security Online Resources

- www.consumer.ftc.gov
- www.onguardonline.gov
- www.staysafeonline.org
- www.us-cert.gov/ncas/tips
- www.stopthinkconnect.org
- www.dhs.gov
- www.identitytheft.gov
- www.haveibeenpwned.org (Email search)
- www.privacyrights.org (Data Breach)