Washington State Fusion Center

Emergency Management Council

Cyber Preparedness for Small and Medium-sized Businesses

February 1, 2018

(U) Tracked by: HSEC-1 and WSFC SIN 4

Overview

<u>Scope</u>: This product is designed to provide an overview of Cyber threats targeting small-to-medium sized businesses and the resources available to those businesses.

<u>Note:</u> This information is the property of the Washington State Fusion Center and may be distributed to law enforcement officials, as well as to public and private sector stakeholders with a **legitimate need-to-know**. Further dissemination to authorized recipients is permitted without prior approval. Precautions should be taken to ensure this information is stored or destroyed in a manner that precludes unauthorized access.

Agenda

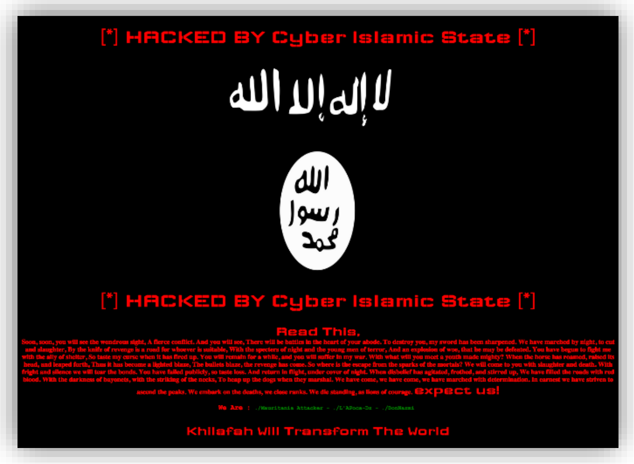
- Threat Actors
- Motivations
- Techniques
- Information They Want
- Dark Web
- Preparedness and Response Resources
- Final Thoughts

Cyber Threat Actors

- State-Sponsored
  - China
  - Russia – APT 28 Cyber Espionage (Sandworm)
  - North Korea
  - Syrian Electric Army (Propaganda)
- Hacktivists – Conduct criminal activity to further agenda
  - Anonymous Collective (DDoS)
  - Islamic Cyber Army
- "Script Kiddies"
- Criminals

Motivations

- Defacement
- Espionage – Competitive advantage
  - Nation/Company advancement
- Disruption – Nuisance, DDoS, or financially motivated (hostage)



[*] HACKED BY Cyber Islamic State [*]

لا إله إلا الله

الله
رسول
محمد

[*] HACKED BY Cyber Islamic State [*]

Read This.

Soon, soon, you will see the wondrous sight, A fierce conflict. And you will see, There will be battles in the heart of your abode. To destroy you, my sword has been sharpened. We have marched by night, to cut and slaughter, By the knife of revenge is a road for whoever is suitable, With the specters of night and the young men of terror, And an explosion of woe, that he may be defeated. You have begun to fight me with the ally of shelter, So taste my curse when it has fired up. You will remain for a while, and you will suffer in my war. With what will you meet a youth made mighty? When the horse has roamed, raised its head, and leaped forth, Thus it has become a lighted blaze, The bullets blaze, the revenge has come. So where is the escape from the sparks of the mortals? We will come to you with slaughter and death. With fright and silence we will tear the bonds. You have failed publicly, so taste loss. And return in flight, under cover of night. When disbelief has agitated, frothed, and stirred up, We have filled the roads with red blood. With the darkness of bayonets, with the striking of the necks, To heap up the dogs when they marshal. We have come, we have come, we have marched with determination. In earnest we have striven to ascend the peaks. We embark on the deaths, we close ranks. We die standing, as lions of courage. expect us!

We Are : ./Mauritania Attacker - ./L'APoca-Dz - ./DonNazmi

Khilafah Will Transform The World

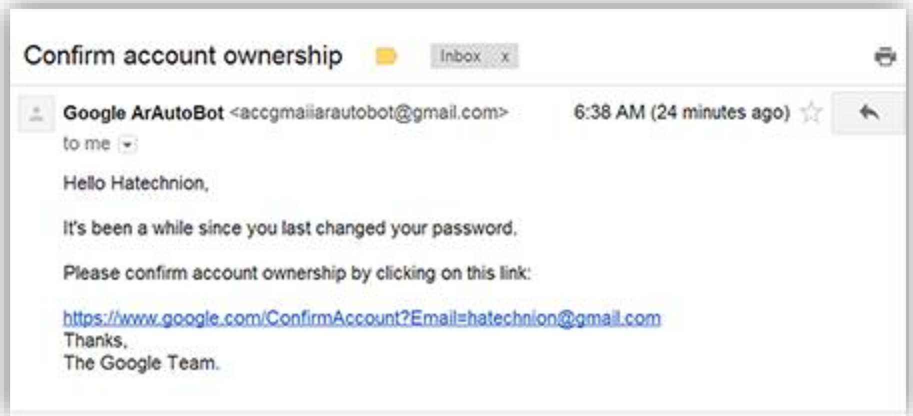
- Financial
  - Laundering; Credential Theft; Ransomware; Underground Market (TOR)
- Inflict Damage and/or Casualties
  - Stuxnet
  - Black Energy - Ukraine Power Grid

Techniques

- DDoS/TDoS
  - Mirai Botnet – East Coast Internet of Things
  - IoTroop
- Doxxing
  - Publicly Releasing Personal Information
- Phishing
  - Sale of Credentials on Dark Web
- Compromise/Deface websites
- Ransomware

Phishing

- Attempts to lure a user to provide private information via:
  - Email
  - Fraudulent Website
  - Telephone



Confirm account ownership

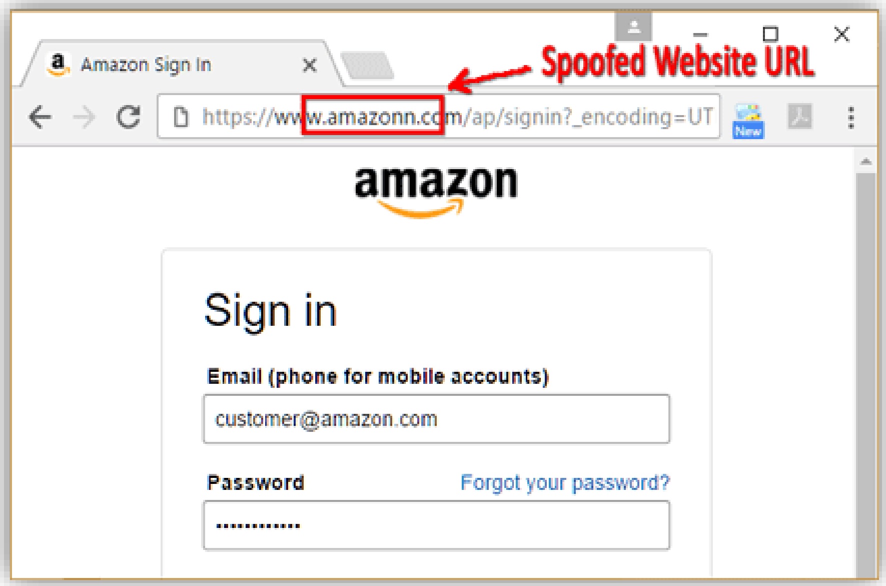
Google ArAutoBot <accgmaiiarautobot@gmail.com> 6:38 AM (24 minutes ago)
to me

Hello Hatechnion,

It's been a while since you last changed your password.

Please confirm account ownership by clicking on this link:

https://www.google.com/ConfirmAccount?Email=hatechnion@gmail.com
Thanks,
The Google Team.



Spoofed Website URL

Sign in

Email (phone for mobile accounts)

customer@amazon.com

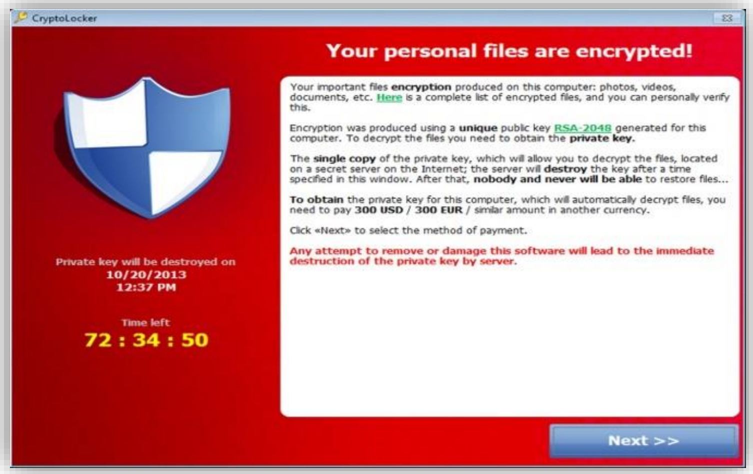
Password Forgot your password?

·············

Ransomware

- Locks computer, files, file names, etc.

- Requires ransom be paid usually within hours or days; otherwise, threatens to permanently delete files.



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 the 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.

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
10/20/2013
12:37 PM

Time left
72 : 34 : 50

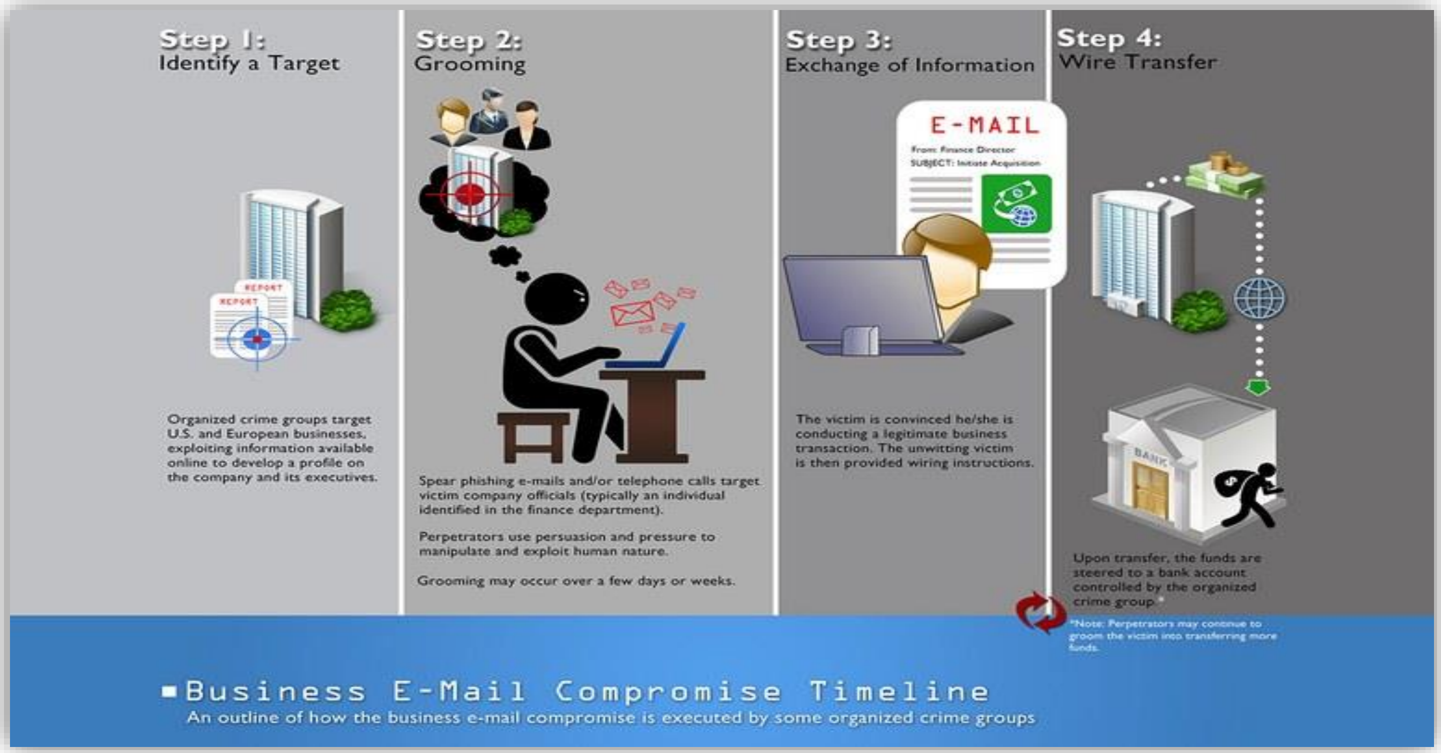
- Infected by opening malicious emails or visiting infected websites.

- Angler Exploit Kit – An exploitation machine that seeks out vulnerabilities on a user’s system.

Ransomware Hostage Rescue Manual

Business Email Compromise

- Email Spoofing
- Requests immediate action from finance dept.
- +1,300% increase in exposed losses since 2015
- 50 States – Hundreds of millions of dollars



Step 1: Identify a Target

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Step 2: Grooming

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

Step 3: Exchange of Information

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4: Wire Transfer

Upon transfer, the funds are steered to a bank account controlled by the organized crime group.*

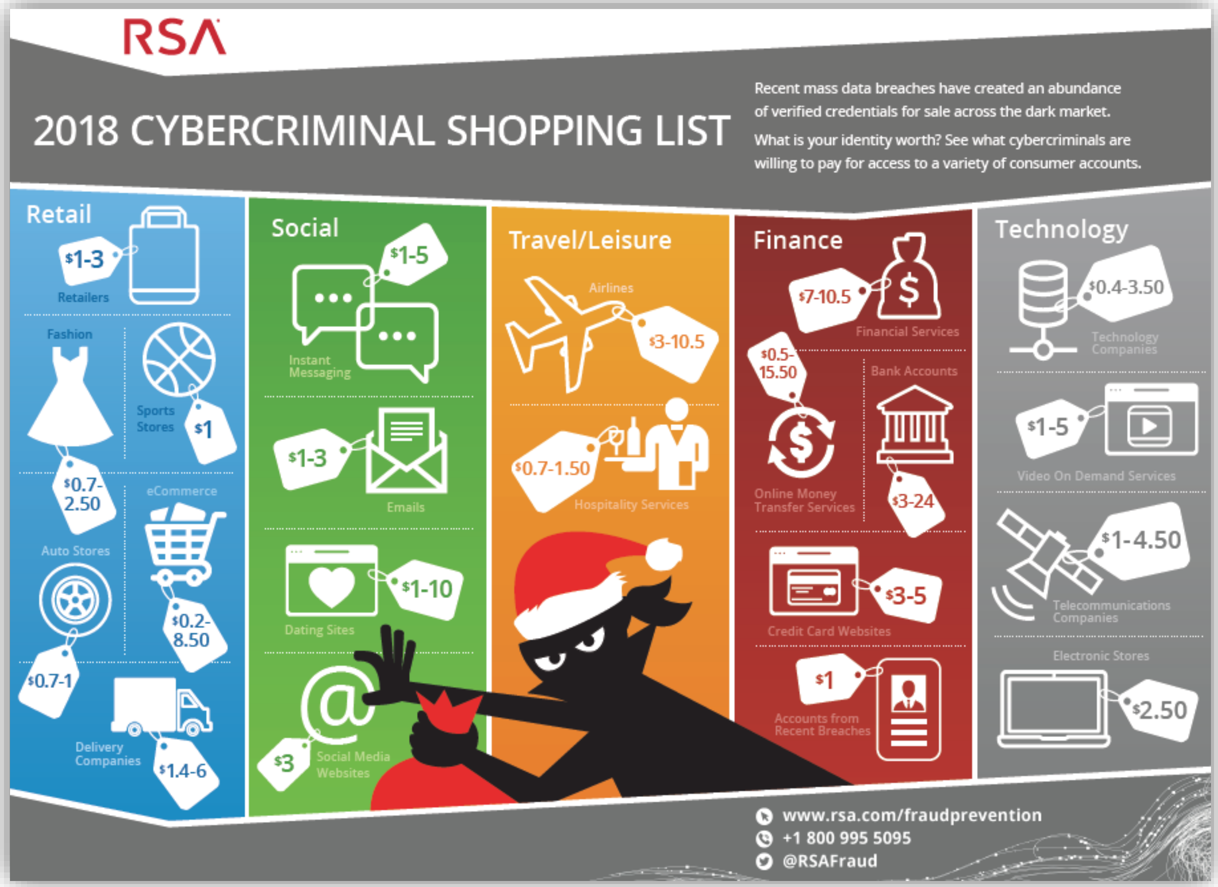
*Note: Perpetrators may continue to groom the victim into transferring more funds.

Business E-Mail Compromise Timeline

An outline of how the business e-mail compromise is executed by some organized crime groups

What do they want?

- Credentials
  - Log-in username and password
- Money…from you
  - Ransom
  - Pay for Service
- Information
  - Medical Data
  - Personal Data
  - Financial Data

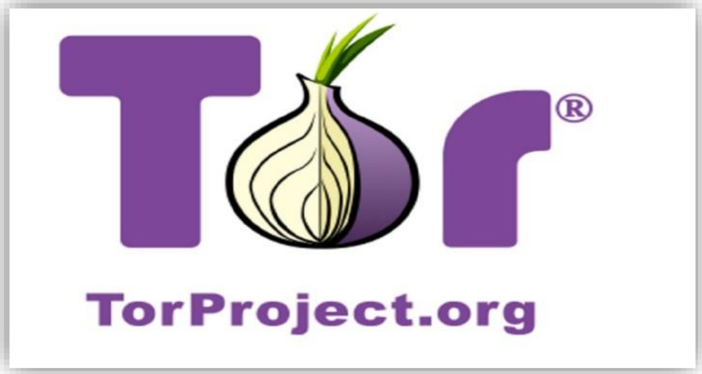


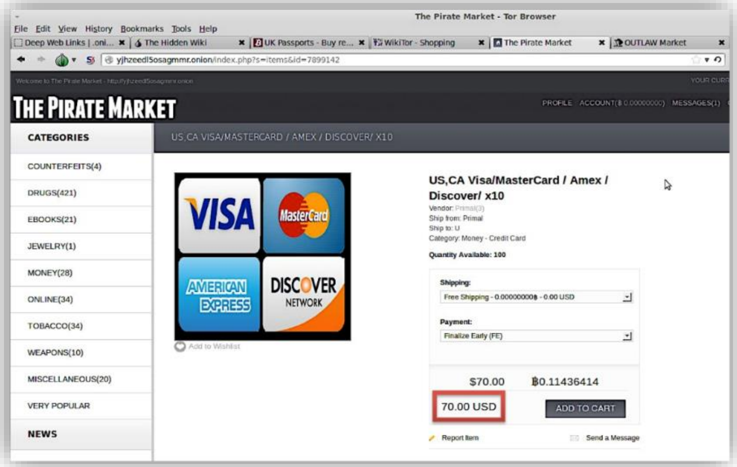
Recent mass data breaches have created an abundance of verified credentials for sale across the dark market.

What is your identity worth? See what cybercriminals are willing to pay for access to a variety of consumer accounts.

Deep and Dark Web

- 0-Day kits for sale
- Malware readily available
- Sell financial/medical information
- Silk Road/Marketplace
- Sell PII
- Illegal goods





US,CA VISA/MASTERCARD / AMEX / DISCOVER/ X10

US,CA Visa/MasterCard / Amex / Discover/ x10

Vendor: Primal(3)
Ship from: Primal
Ship to: U
Category: Money - Credit Card

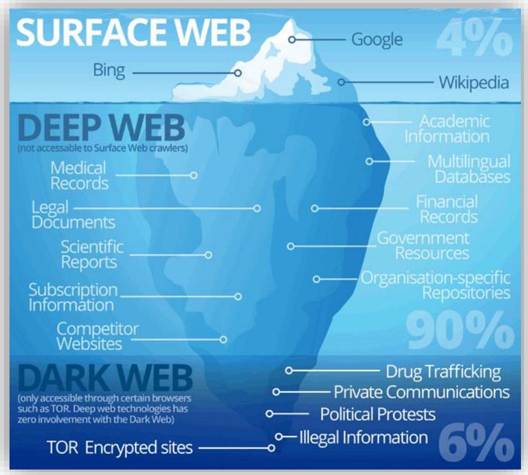
Quantity Available: 100

Shipping: Free Shipping - 0.00000000฿ - 0.00 USD

Payment: Finalize Early (FE)

$70.00 ฿0.11436414

70.00 USD



WASHINGTON STATE FUSION CENTER
WSFC

Resources

- WSFC
- MS-ISAC
- USSS
- FBI
  - Infragard
- IC3
- DHS
- NIST Framework

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

UNITED STATES SECRET SERVICE

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

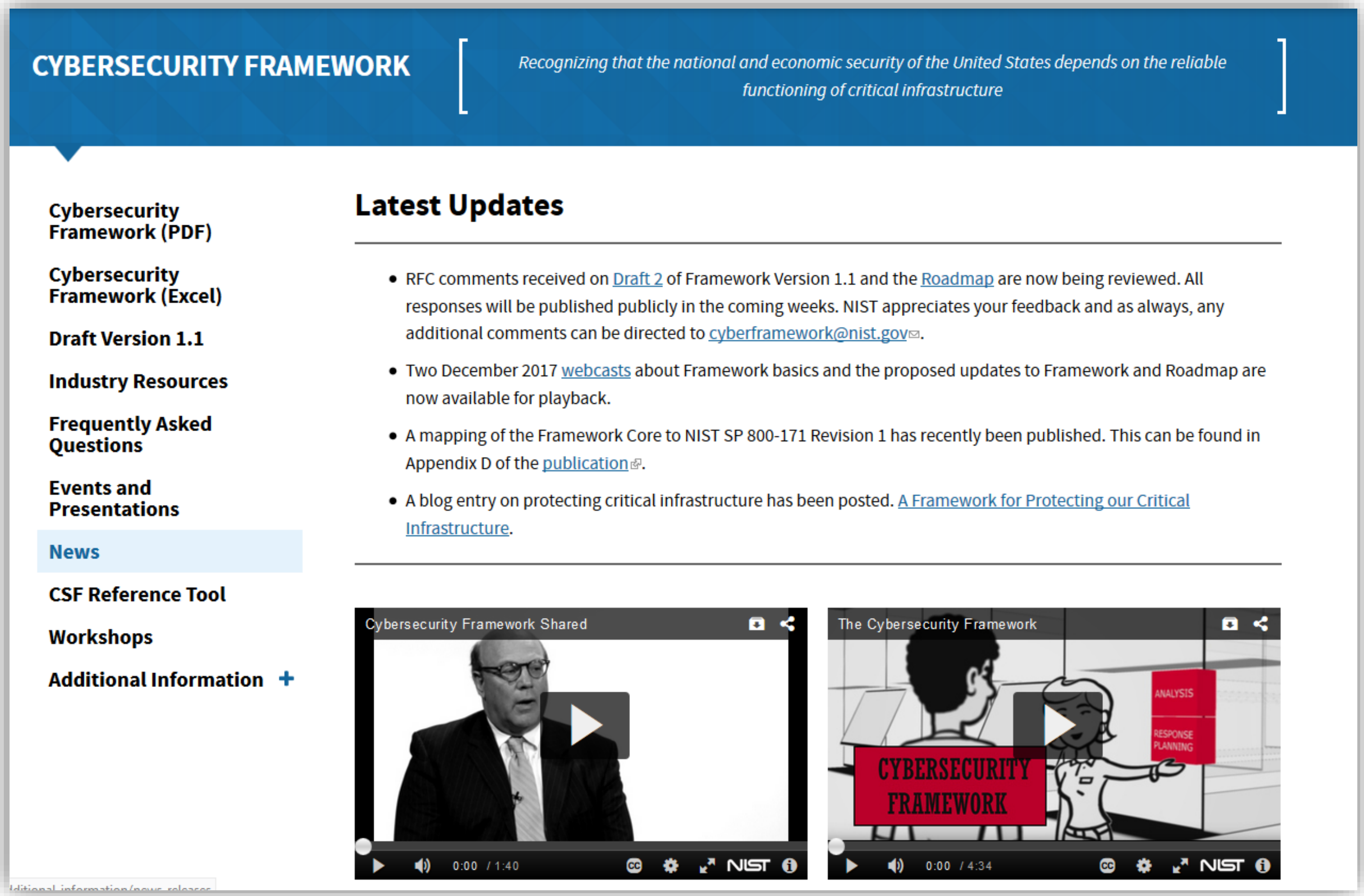
U.S. DEPARTMENT OF HOMELAND SECURITY

FBI CYBER DIVISION
IDENTIFY · PURSUE · DEFEAT

FEDERAL BUREAU OF INVESTIGATION
IC3
INTERNET CRIME COMPLAINT CENTER

INFRAGARD
PARTNERSHIP FOR PROTECTION

NIST Framework



CYBERSECURITY FRAMEWORK

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure

- Cybersecurity Framework (PDF)
- Cybersecurity Framework (Excel)
- Draft Version 1.1
- Industry Resources
- Frequently Asked Questions
- Events and Presentations
- News
- CSF Reference Tool
- Workshops
- Additional Information +

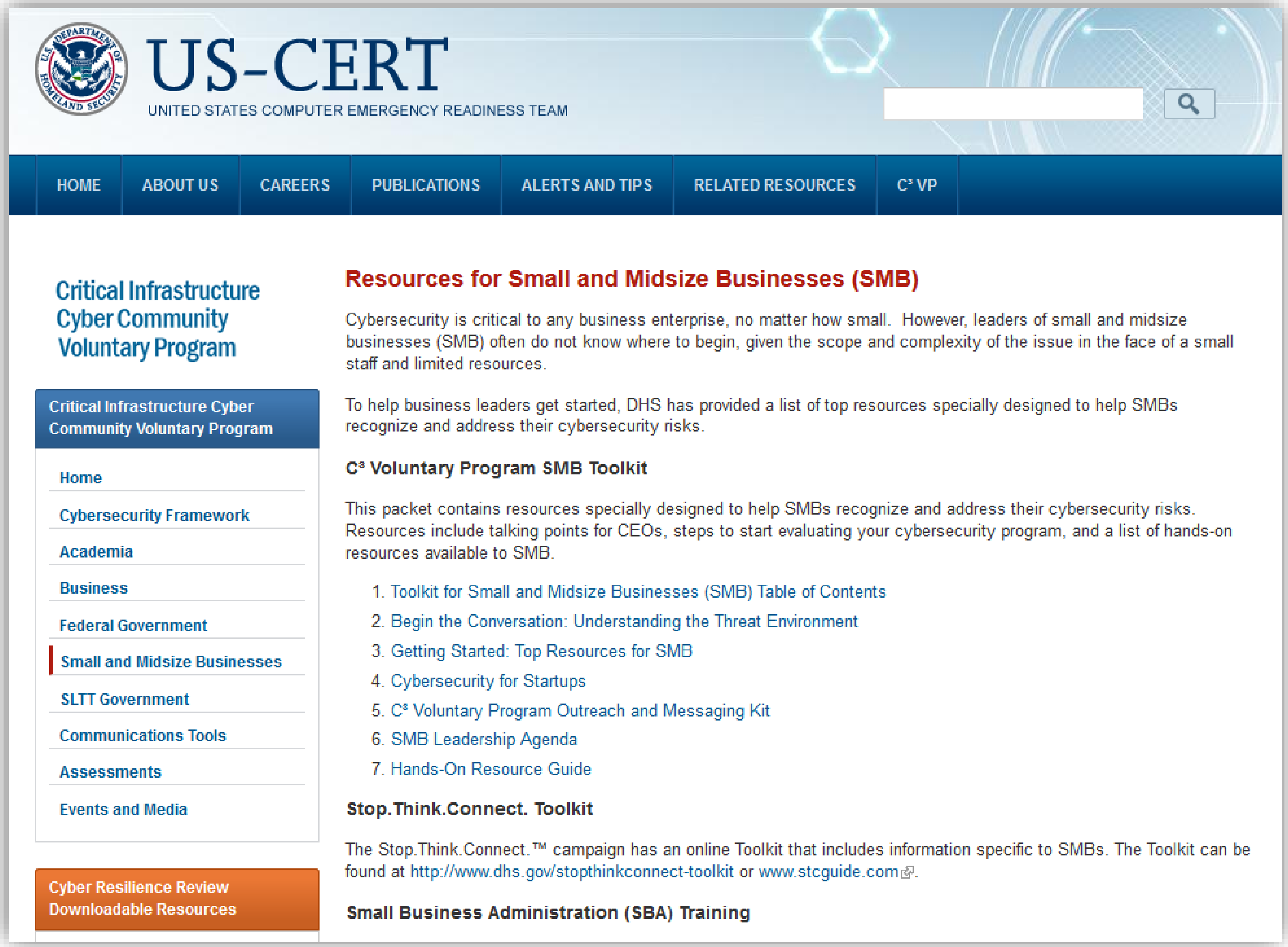
Latest Updates

- RFC comments received on Draft 2 of Framework Version 1.1 and the Roadmap are now being reviewed. All responses will be published publicly in the coming weeks. NIST appreciates your feedback and as always, any additional comments can be directed to cyberframework@nist.gov.
- Two December 2017 webcasts about Framework basics and the proposed updates to Framework and Roadmap are now available for playback.
- A mapping of the Framework Core to NIST SP 800-171 Revision 1 has recently been published. This can be found in Appendix D of the publication.
- A blog entry on protecting critical infrastructure has been posted. A Framework for Protecting our Critical Infrastructure.

Cybersecurity Framework Shared
0:00 / 1:40
NIST
The Cybersecurity Framework
ANALYSIS
RESPONSE PLANNING
CYBERSECURITY FRAMEWORK
0:00 / 4:34
NIST
dditional-information/news-releases

https://www.nist.gov/cyberframework/industry-resources

C³ Voluntary Program



Critical Infrastructure Cyber Community Voluntary Program

Critical Infrastructure Cyber Community Voluntary Program

- Home
- Cybersecurity Framework
- Academia
- Business
- Federal Government
- Small and Midsize Businesses
- SLTT Government
- Communications Tools
- Assessments
- Events and Media

Cyber Resilience Review Downloadable Resources

Resources for Small and Midsize Businesses (SMB)

Cybersecurity is critical to any business enterprise, no matter how small. However, leaders of small and midsize businesses (SMB) often do not know where to begin, given the scope and complexity of the issue in the face of a small staff and limited resources.

To help business leaders get started, DHS has provided a list of top resources specially designed to help SMBs recognize and address their cybersecurity risks.

C³ Voluntary Program SMB Toolkit

This packet contains resources specially designed to help SMBs recognize and address their cybersecurity risks. Resources include talking points for CEOs, steps to start evaluating your cybersecurity program, and a list of hands-on resources available to SMB.

1. Toolkit for Small and Midsize Businesses (SMB) Table of Contents
2. Begin the Conversation: Understanding the Threat Environment
3. Getting Started: Top Resources for SMB
4. Cybersecurity for Startups
5. C³ Voluntary Program Outreach and Messaging Kit
6. SMB Leadership Agenda
7. Hands-On Resource Guide

Stop.Think.Connect. Toolkit

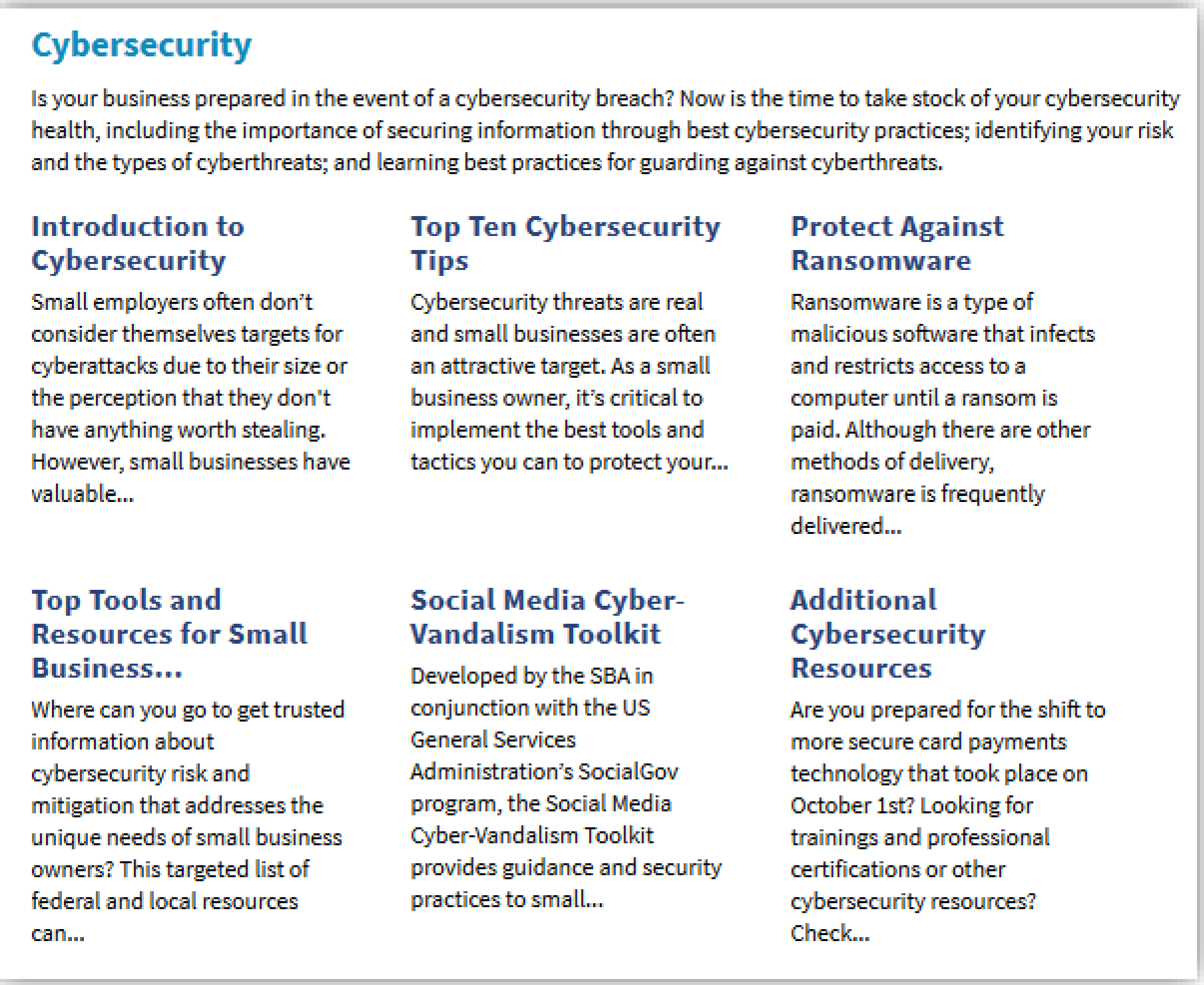
The Stop.Think.Connect.™ campaign has an online Toolkit that includes information specific to SMBs. The Toolkit can be found at http://www.dhs.gov/stopthinkconnect-toolkit or www.stcguide.com.

Small Business Administration (SBA) Training

https://www.us-cert.gov/ccubedvp/smb

Small Business Administration

SBA
U.S. Small Business Administration



Cybersecurity

Is your business prepared in the event of a cybersecurity breach? Now is the time to take stock of your cybersecurity health, including the importance of securing information through best cybersecurity practices; identifying your risk and the types of cyberthreats; and learning best practices for guarding against cyberthreats.

Introduction to Cybersecurity

Small employers often don't consider themselves targets for cyberattacks due to their size or the perception that they don't have anything worth stealing. However, small businesses have valuable...

Top Ten Cybersecurity Tips

Cybersecurity threats are real and small businesses are often an attractive target. As a small business owner, it's critical to implement the best tools and tactics you can to protect your...

Protect Against Ransomware

Ransomware is a type of malicious software that infects and restricts access to a computer until a ransom is paid. Although there are other methods of delivery, ransomware is frequently delivered...

Top Tools and Resources for Small Business...

Where can you go to get trusted information about cybersecurity risk and mitigation that addresses the unique needs of small business owners? This targeted list of federal and local resources can...

Social Media Cyber-Vandalism Toolkit

Developed by the SBA in conjunction with the US General Services Administration's SocialGov program, the Social Media Cyber-Vandalism Toolkit provides guidance and security practices to small...

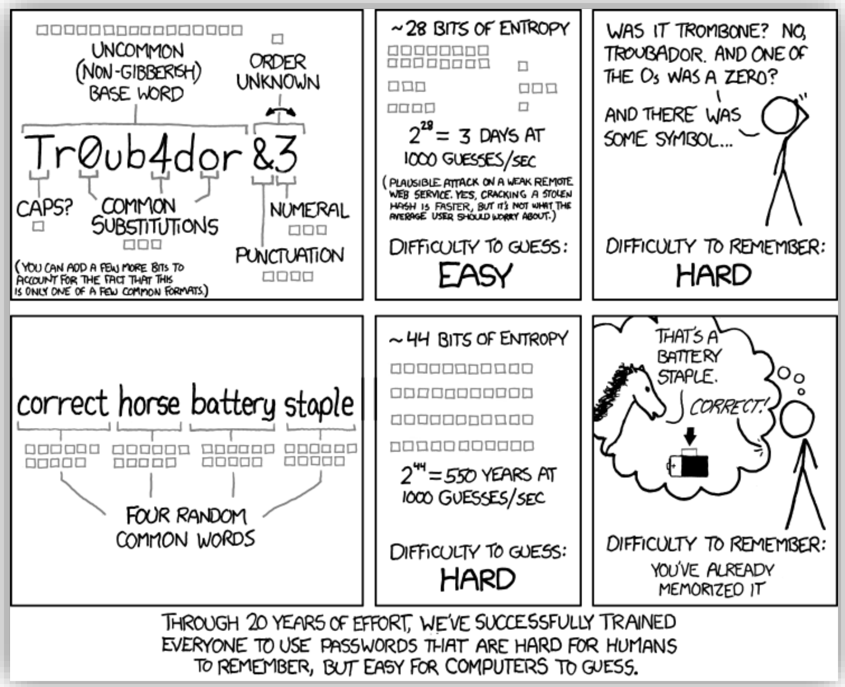
Additional Cybersecurity Resources

Are you prepared for the shift to more secure card payments technology that took place on October 1st? Looking for trainings and professional certifications or other cybersecurity resources? Check...

https://www.sba.gov/managing-business/cybersecurity

Final Thoughts

- Threat actors will continue to seek vulnerabilities = PATCH!
- Employees will continue to click on links to get a “Free iPad”
- Have a policy in place to verify wire transfer requests
- Practice good cyber hygiene
  - Change default username and passwords
  - Use strong passwords and a password manager
  - Use multi-factor authentication
- Routinely backup data


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

QUESTIONS ?

WASHINGTON STATE ★ FUSION CENTER ★

WSFC