CyberSecure MY BUSINESS

PLAN. PROTECT. RESPOND.

National Cyber Security Alliance

NATIONAL CYBERSECURITY ALLIANCE

NATIONAL CYBERSECURITY ALLIANCE

Board Companies

ADP aetna at&t Bank of America BARCLAYS

CDK Global CISCO COMCAST eset f Google

intel LifeLock Logical Operations mastercard Microsoft

NXP PayPal PKWARE Raytheon RSA

salesforce SANS SECURING THE HUMAN Symantec. TeleSign VISA WELLS FARGO

How do you define Cybersecurity?

Define Cybersecurity

“The ability to protect or defend the use of cyberspace from cyber attack.” National Institute of Science and Technology (NIST)

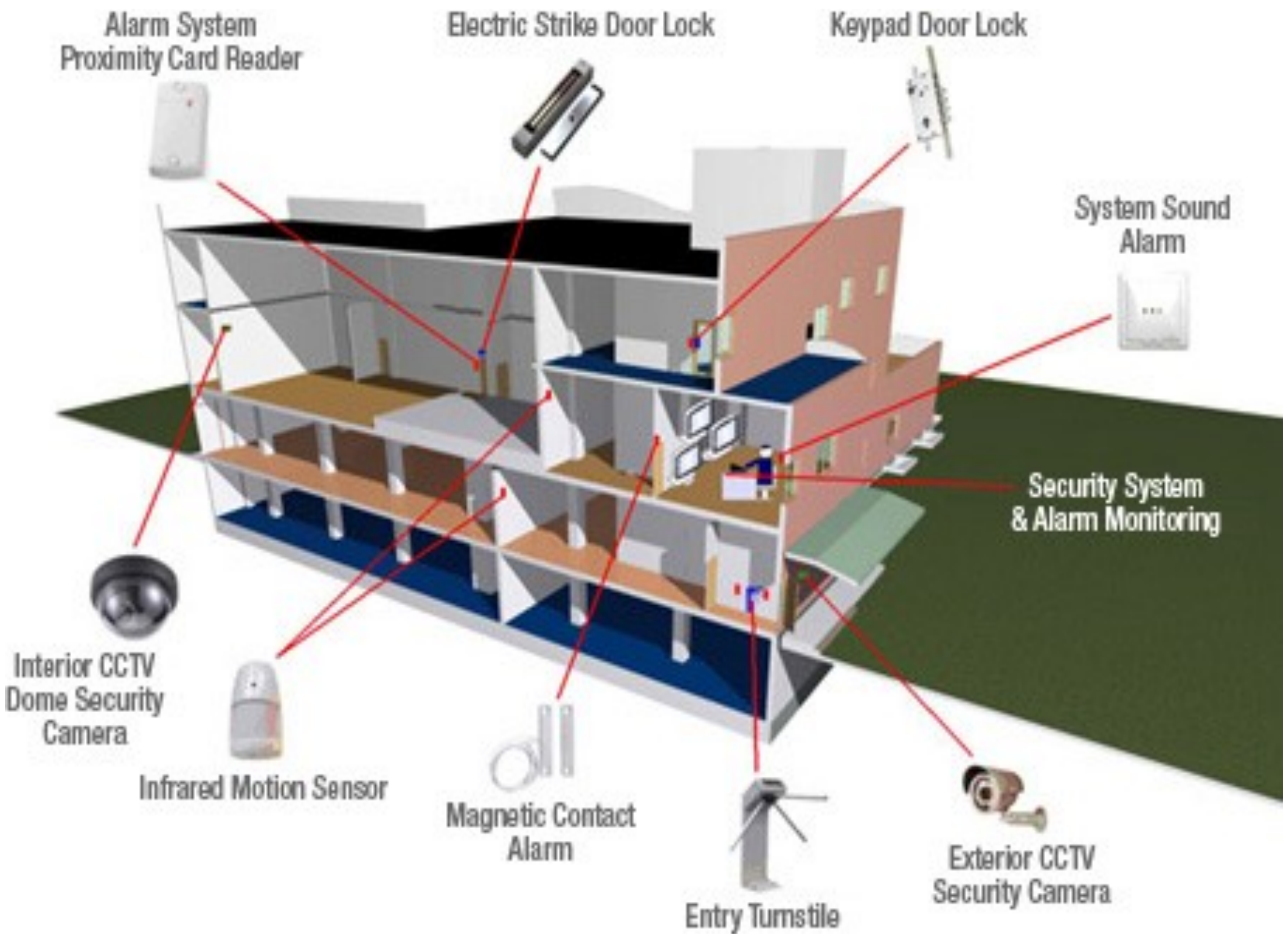
“Enabling people and businesses to do more online with trust and confidence.” NCSA

Program Overview

Today’s Discussion

- What are the threats
- NIST 5-Step Approach to Cybersecurity
- 5-Step Scenario
- Federal Trade Commission “Start with Security”
- Resources

Physical Office Security



Physical Security vs. Cybersecurity

Keypad Door Lock = Authentication

Interior Camera = Intrusion Detection System

Electronic Strike Door Lock = Firewall

Exterior Camera = Anti-Virus Protection

CyberSecure MY BUSINESS

THREATS

What are the threats?

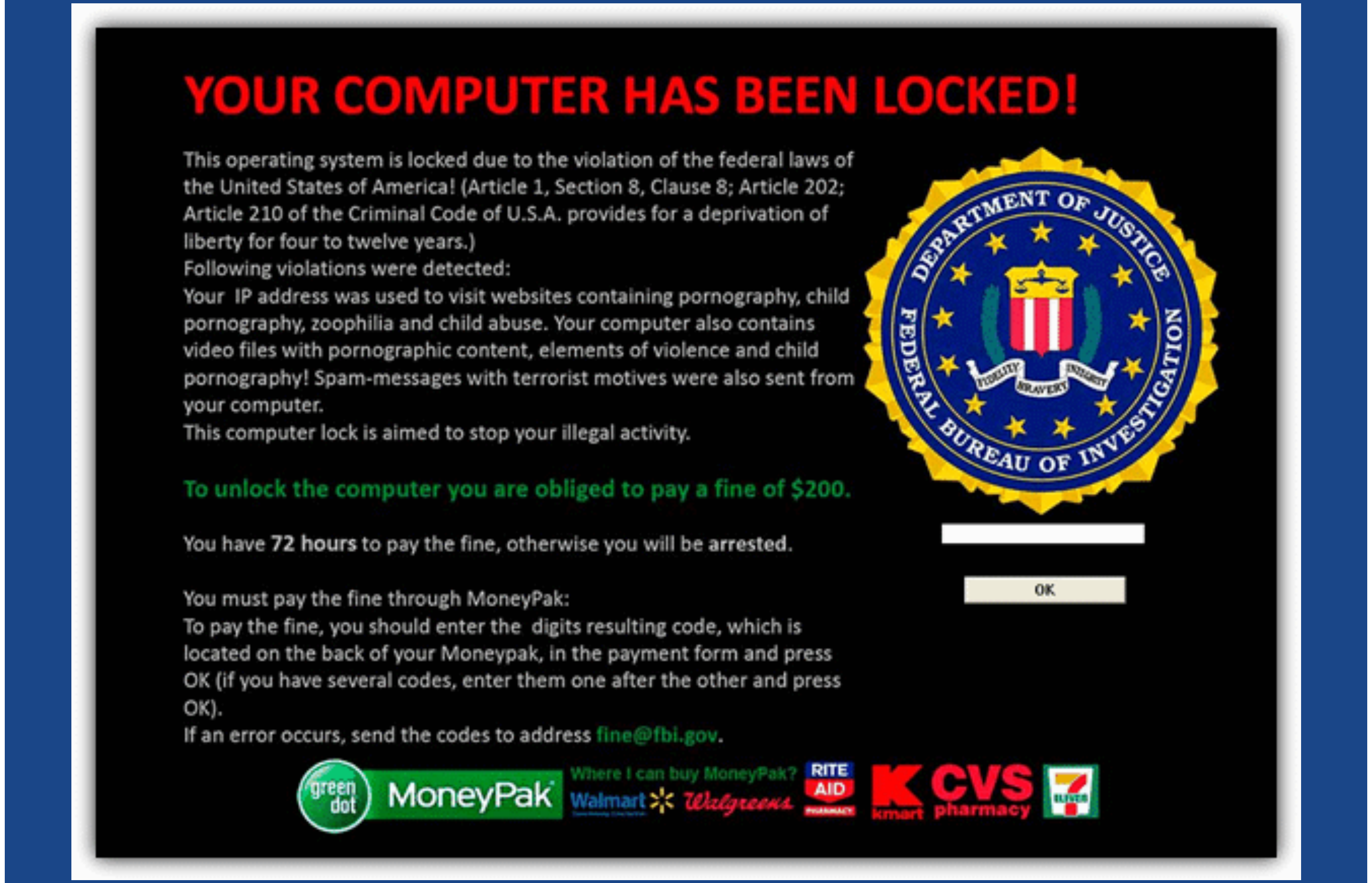
ONLY NINE CATEGORIES

The threats facing businesses fall into these categories

- Physical Theft and Loss
- Payment Card Skimmers
- Point-of Sale Intrusions
- Crimeware (Malware/Ransomware)
- Web Apps
- Denial of Service
- Cyber-espionage
- Insider and Privilege Misuse
- Miscellaneous Errors

Verizon Data Breach Report 2016

Ransomware



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

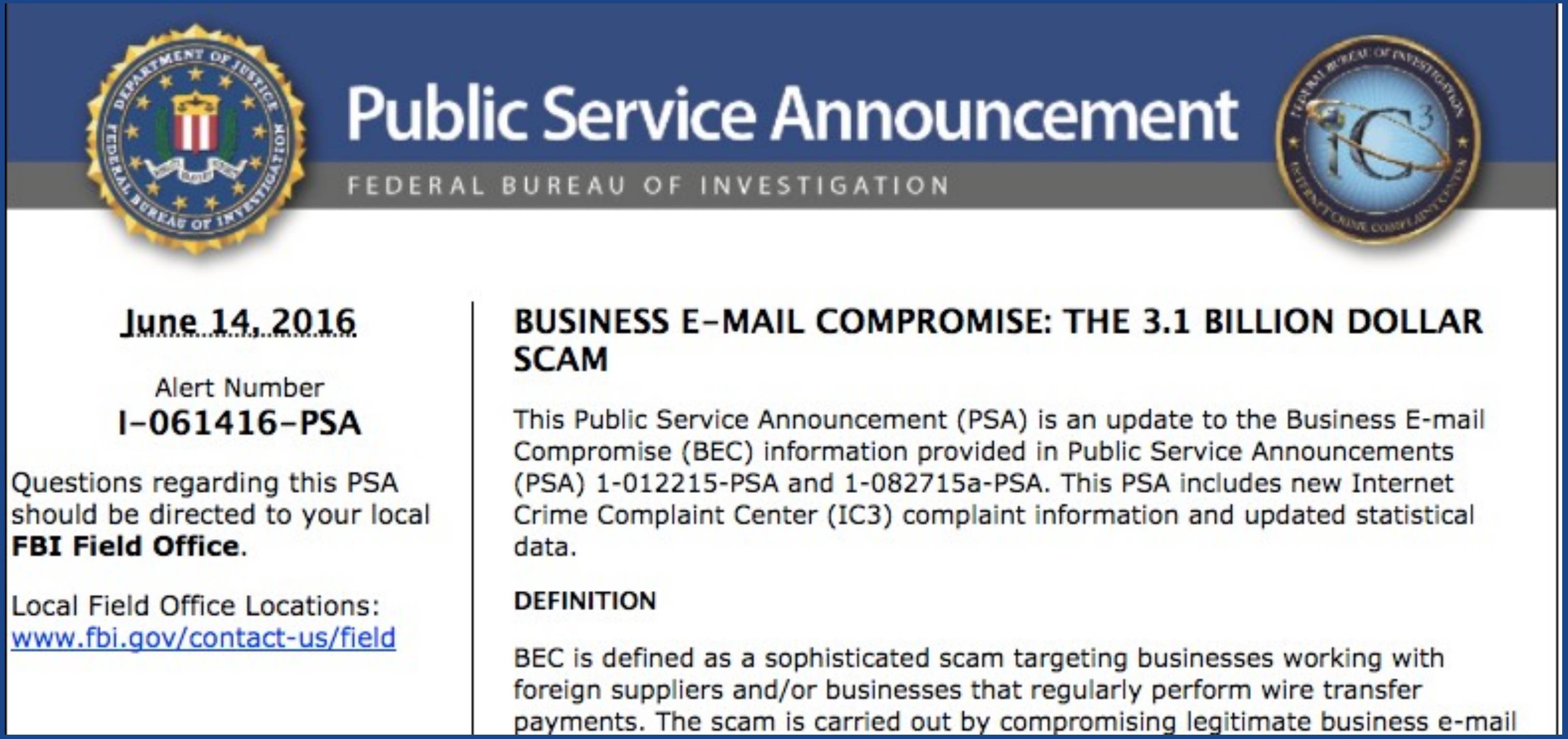
To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through MoneyPak:
To pay the fine, you should enter the digits resulting code, which is located on the back of your Moneypak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

OK

Business Email Compromise



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

June 14, 2016

Alert Number
I-061416-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations:
www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE: THE 3.1 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to the Business E-mail Compromise (BEC) information provided in Public Service Announcements (PSA) 1-012215-PSA and 1-082715a-PSA. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data.

DEFINITION

BEC is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail

WWW.IC3.GOV

CyberSecure MY BUSINESS

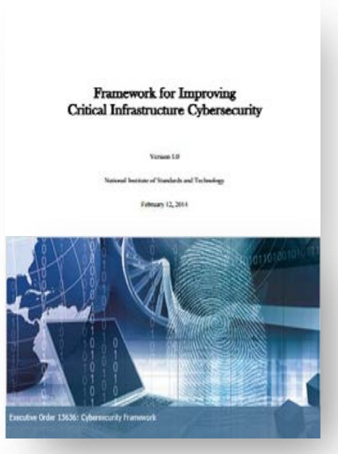
5-Step Solution

NIST 5-Step Approach

The NIST Cybersecurity Framework Covers 5 Major Functions

This internationally recognized framework gives businesses a way to think about cybersecurity and was created by public and private sector working together.

1. IDENTIFY assets you need to protect
2. PROTECT assets and limit impact
3. DETECT security problems
4. RESPOND to an incident
5. RECOVER from an incident



Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

Executive Order 13636: Cybersecurity Framework

CyberSecure
MY BUSINESS

5-Step Approach for Fire Prevention – Page 3

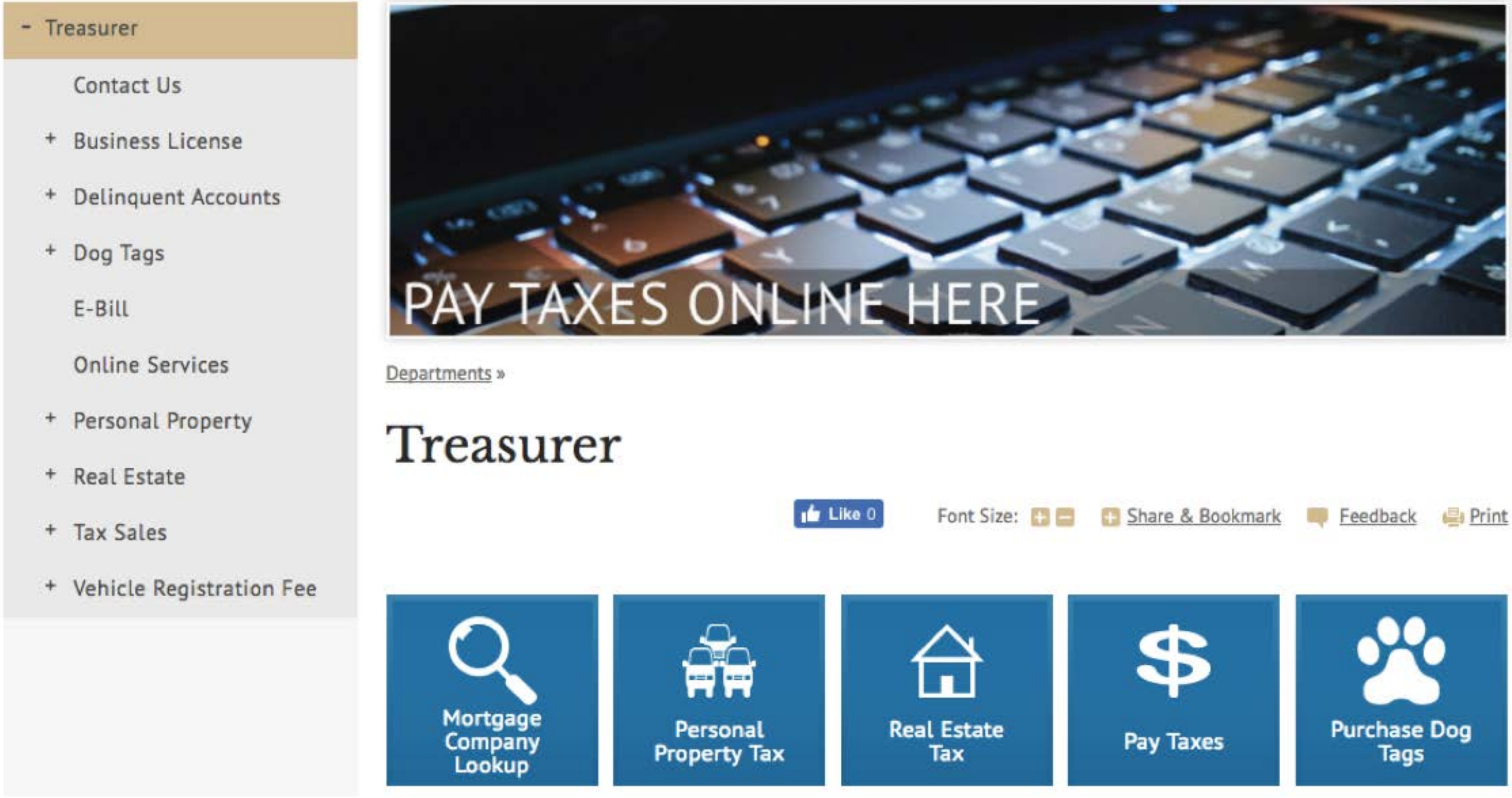
IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Building Assets And Staff				

5-Step Approach for Fire Prevention

Identify	Protect	Detect	Respond	Recover
Building Assets And Staff	Fire Exits Smoke Alarms Label Inventory	Alarm Goes Off	Meet at Mailbox Call 9-1-1 Call Insurance	Purchase New Items Notify Customers Clean up Smoke and Water Damage

Let’s Try It!

A Real-Life Scenario – County Treasurer



CyberSecure
MY BUSINESS

Step 1: Identify

Exercise: Page 3

What are the most important data and technology assets the Treasurer’s Office needs to protect from cyber attacks?

STEP 1 - IDENTIFY

Identify	Protect	Detect	Respond	Recover
Email Staff accesses financial accounts, state and federal data				

CyberSecure
MY BUSINESS

Inventory List Sample

Physical Devices

- Computers
- Phones
- Servers
- Tablets
- Hard drives

Data

- Social security numbers
- Health data
- Payment data
- Personal information

Location/Access

- Administrators
- Room
- IP addresses

CyberSecure
MY BUSINESS

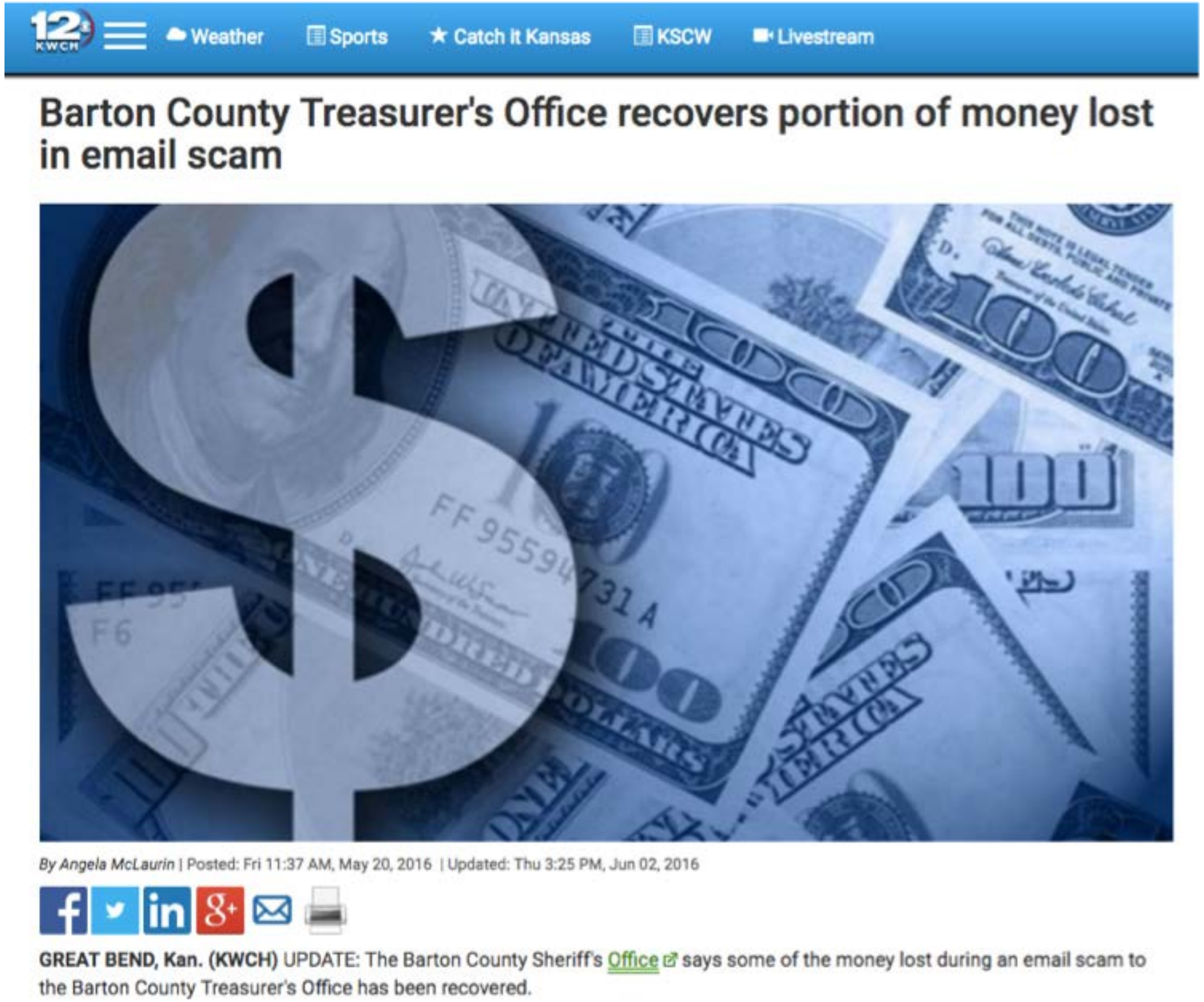
Step 1: Identify

Exercise: Page 4

What are the most important data and technology assets YOU need to protect from cyber attacks?

THE BREACH HAPPENS

Business Email Compromise – Where did the money go?



Barton County Treasurer's Office recovers portion of money lost in email scam

By Angela McLaurin | Posted: Fri 11:37 AM, May 20, 2016 | Updated: Thu 3:25 PM, Jun 02, 2016

GREAT BEND, Kan. (KWCH) UPDATE: The Barton County Sheriff's Office says some of the money lost during an email scam to the Barton County Treasurer's Office has been recovered.

CyberSecure
MY BUSINESS

How did this happen?

Social Engineering/Phishing

How much are you/your staff sharing online?

Do you scrutinize email requests?

Are there protocols set up to address suspicious requests?

Step 2: Protect

Exercise: Page 5

What could the Treasurer’s Office be doing to protect his data and devices?

STEP 2 - PROTECT

Identify	Protect	Detect	Respond	Recover
Email Contains dates, times, accounts for wire transactions	Add strong authentication to email Train staff often Limit what is shared online Establish protocols with clients early			

Let’s Talk About Passwords

Passwords don’t work

Most popular is still “123456” or “password”

We don’t store them safely

Make a Passphrase

Example: I like to eat ice cream on Sundays

Passphrase:

ILikeToEatIceCreamOn$unday$

Add one letter at the end of phrase that matches the URL

Authentication Required

Passwords/passphrases can be stolen

Authentication is critical to add to email, social media etc.

CyberSecure MY BUSINESS

Step 3: Detect

Exercise: Page 5

What could the Treasurer’s Office have done to detect that something was wrong before the breach?

STEP 3 - DETECT

Identify	Protect	Detect	Respond	Recover
Email Contains dates, times, accounts for wire transactions	Add strong authentication to email Train staff often Limit what is shared online Establish protocols with clients early	Use intrusion detection system to flag bad emails Regular non-electronic comms Scrutinize email requests		

CyberSecure
MY BUSINESS

Step 4: Respond

Exercise: Page 6

How could the Treasurer’s Office respond once they learn of the breach?

Two areas – fix the issue and business continuity

STEP 4 - RESPOND

Identify	Protect	Detect	Respond	Recover
Email Contains dates, times, accounts for wire transactions	Add strong authentication to email Train staff often Limit what is shared online Establish protocols with clients early	Use intrusion detection system to flag bad emails Regular non-electronic comms Scrutinize email requests	Call financial institution immediately Contact local FBI File complaint with IC3.GOV	

Step 5: Recover

Exercise: Page 6

What does recovery look like?

STEP 5 - RECOVER

Identify	Protect	Detect	Respond	Recover
Email Contains dates, times, accounts for wire transactions	Add strong authentication to email Train staff often Limit what is shared online Establish protocols with clients early	Use intrusion detection system to flag bad emails Regular non-electronic comms Scrutinize email requests	Call financial institution immediately Contact local FBI File complaint with IC3.GOV	Who is responsible for the lost money? Depends on state laws Reputation management

CyberSecure MY BUSINESS

Avoid Becoming a Business Email Compromise Victim

- ADD STRONG AUTHENTICATION!
- Train employees in security principles
- Protect information, computers, and networks from viruses, spyware etc.
- Delete or block spam
- Verify email sources: Digital signatures, check addresses, verify by phone
- Forward vs. reply: Ensure typing the correct address
- Keep a Clean Machine: Update software regularly
- Have IT support you can trust and interact with regularly

Back-up, Back-up, Back-up – *Page 7*

3-2-1 Back-Up Rule

- 3 back-up copies
- 2 different media
- 1 offline and in a separate location

Exercise: What is your back-up plan? Take a few minutes to write a plan or confirm the plan you already have.

Cloud Services

Make a list of cloud services you use.

Ask about how they handle:

- Maintenance
- Patching
- Firewall
- Encryption
- Backup/Restore

FEDRAMP.GOV

5-Steps with Cloud Providers

Identify	Protect	Detect	Respond	Recover
Vendor Support	Vendor Support	Vendor Support	Vendor Support	Vendor Support

CyberSecure MY BUSINESS

Breach Notification

Make a list of contact you need when a breach happens.

- Train employees to identify and report breaches
- Establish financial institutions you need to notify
- Reporting obligations differ depending on state law
  - 49 states have reporting laws
  - National Conference of State Legislators
  - www.ncsl.org

Consult your counsel BEFORE a breach!

CyberSecure MY BUSINESS

Policy Examples

What polices do you already have in place?

Acceptable use (of information technology)
All device/network users will read and sign an access and use agreement.

Training and awareness
All staff will participate in cyber security education program.

Physical security
Devices must be secured when leaving your desk or traveling.

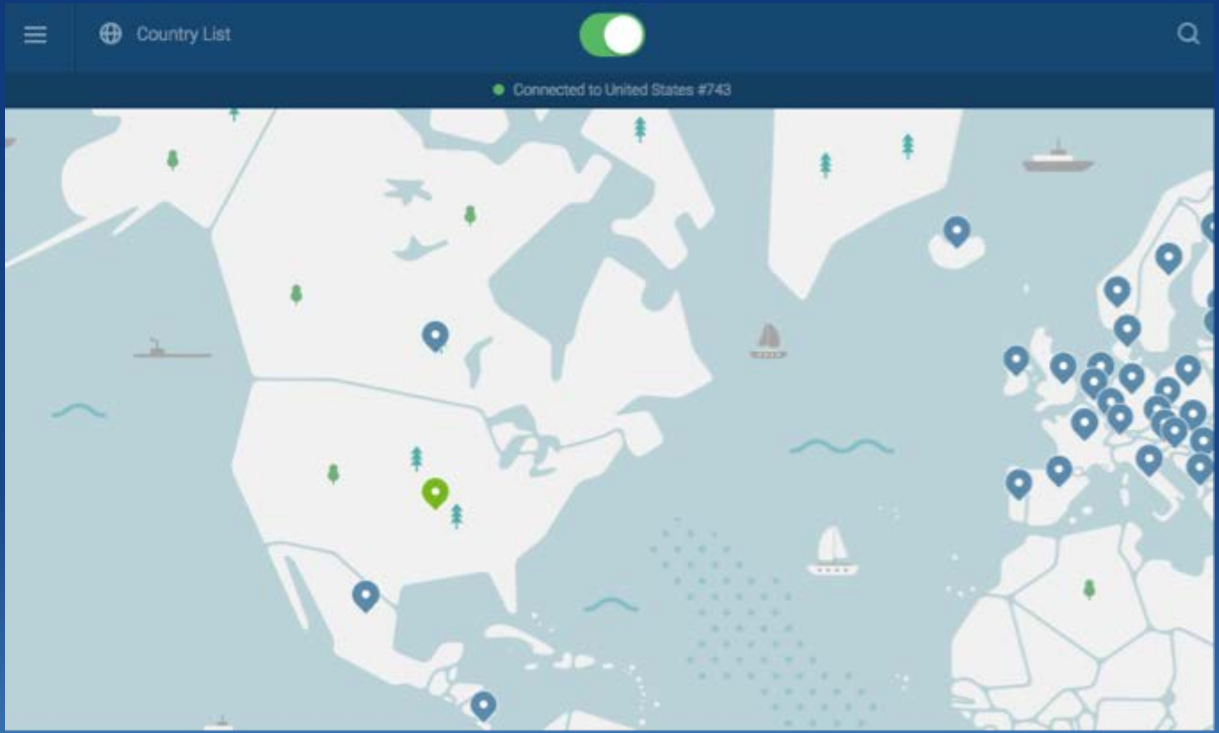
Password and authentication
Passphrases must (be strong and unique for work) and authentication enabled on all email accounts.

Personnel security
All personnel data will be protected from viewing or changing by unauthorized persons.

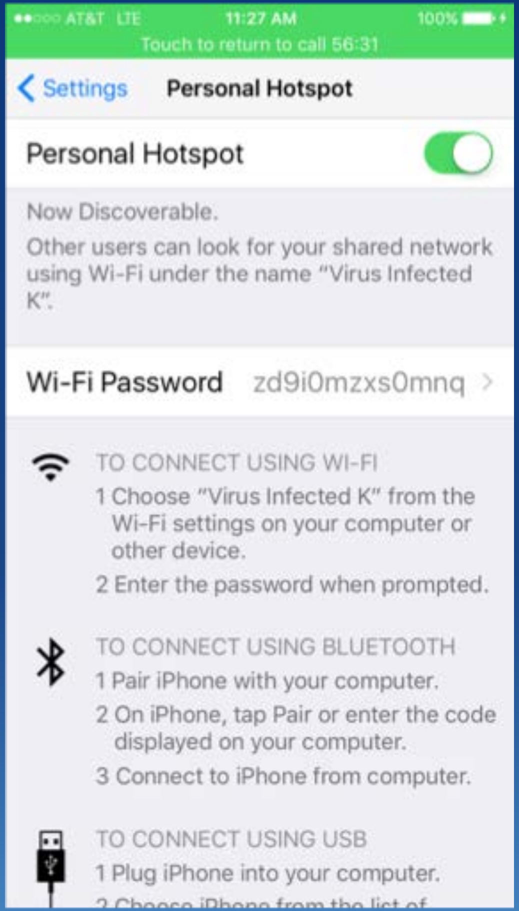
Email Usage
Personal or sensitive data may not be sent in email.

PUBLIC WIFI SECURITY

VPN



Hotspot


●●○○○ AT&T LTE 11:27 AM 100%

Touch to return to call 56:31

Settings Personal Hotspot

Personal Hotspot

Now Discoverable.
Other users can look for your shared network using Wi-Fi under the name “Virus Infected K”.

Wi-Fi Password zd9i0mzxs0mnq

TO CONNECT USING WI-FI

1 Choose “Virus Infected K” from the Wi-Fi settings on your computer or other device.

2 Enter the password when prompted.

TO CONNECT USING BLUETOOTH

1 Pair iPhone with your computer.

2 On iPhone, tap Pair or enter the code displayed on your computer.

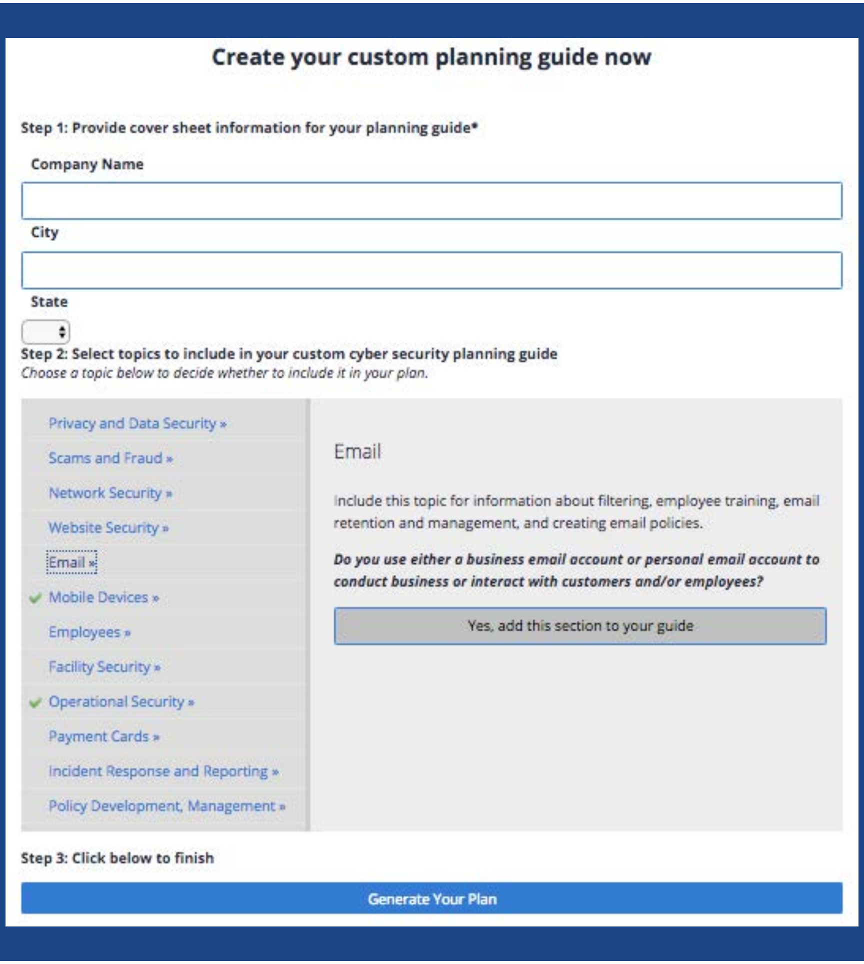
3 Connect to iPhone from computer.

TO CONNECT USING USB

1 Plug iPhone into your computer.

2 Choose iPhone from the list of

FCC Response Plan



Create your custom planning guide now

Step 1: Provide cover sheet information for your planning guide*

Company Name

City

State

Step 2: Select topics to include in your custom cyber security planning guide
Choose a topic below to decide whether to include it in your plan.

- Privacy and Data Security »
- Scams and Fraud »
- Network Security »
- Website Security »
- Email »
- ✓ Mobile Devices »
- Employees »
- Facility Security »
- ✓ Operational Security »
- Payment Cards »
- Incident Response and Reporting »
- Policy Development, Management »

Email

Include this topic for information about filtering, employee training, email retention and management, and creating email policies.

Do you use either a business email account or personal email account to conduct business or interact with customers and/or employees?

Step 3: Click below to finish

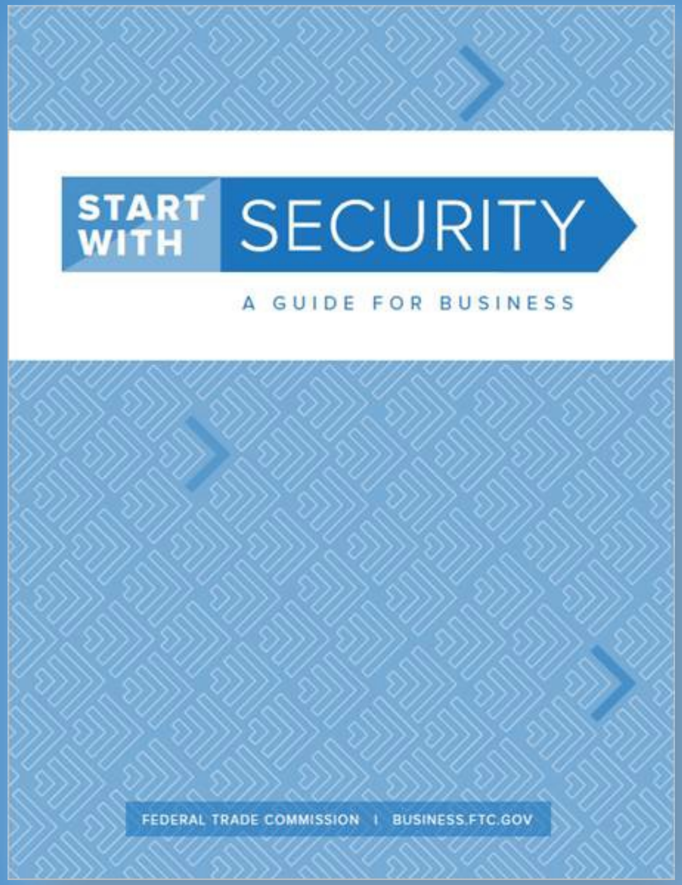
- Privacy and Data Security
- Scams and Fraud
- Network Security
- Website Security
- Email
- Mobile Devices
- Employees
- Etc.

CyberSecure
MY BUSINESS

CyberSecure MY BUSINESS

Don’t be overwhelmed …Resources are available

Federal Trade Commission (FTC)
“Start with Security”



START WITH SECURITY

A GUIDE FOR BUSINESS

FEDERAL TRADE COMMISSION | BUSINESS.FTC.GOV

FROM: Start with Security: A Guide for Business, FTC

1. Start with Security

Factor security into all decision making

- What kinds of information do you collect?
- How long do you keep it?
- Who do you share it with?
- Who has access?

Lead by example to create a culture of security at work

FROM: Start with Security: A Guide for Business, FTC

CyberSecure MY BUSINESS

2. Control Access to Data Sensibly

BEST PRACTICES

- Restrict access to sensitive data to those who need it for job duties
- Minimize administrative privileges on your network

FTC CASE: TWITTER

Granting administrative access to most employees increased risk of eventual breach.

FROM: Start with Security: A Guide for Business, FTC

3. Require Secure “Passphrases” and Authentication

BEST PRACTICES

- Store passphrases securely and add strong authentication
- Guard against brute force attacks

FTC CASE: GUIDANCE SOFTWARE

Network credentials stored in clear text helped hacker access credit card information.

FROM: Start with Security: A Guide for Business, FTC

CyberSecure MY BUSINESS

4. Store Sensitive Information Securely and Protect During Transmission

BEST PRACTICES

- Ensure staff handling sensitive data understand how to protect it
- Encrypt sensitive information stored on network and during transmission

FTC CASE: SUPERIOR MORTGAGE

Sensitive customer data encrypted on collection at website was decrypted and emailed to branch offices.

FROM: Start with Security: A Guide for Business, FTC

CyberSecure MY BUSINESS

5. Segment your network and monitor who's trying to get in and out

BEST PRACTICES

- Not all computers need to communicate
- Monitor network activity

FTC CASE: DSW

Computers were not prevented from connecting across in-store and corporate networks.

FROM: Start with Security: A Guide for Business, FTC

CyberSecure MY BUSINESS

6. Secure Remote Access to Your Network

BEST PRACTICES

Before enabling remote access:

- Assess client/vendor security
- Ensure staff computers/devices are secure
- Restrict access to known IP addresses grant temporary access as needed

FTC CASE: LIFELOCK

No antivirus programs installed on staff computers used to remotely access network.

FROM: Start with Security: A Guide for Business, FTC

CyberSecure MY BUSINESS

7. Apply Sound Security Practices When Developing New Products

BEST PRACTICES

- Train your engineers in secure coding
- Verify that privacy and security features work
- Test for common vulnerabilities

FTC CASE: SNAPCHAT

The company advertised that messages would "disappear forever," but they failed to ensure the accuracy of that claim.

FROM: Start with Security: A Guide for Business, FTC

CyberSecure MY BUSINESS

8. Make Sure Service Providers Implement Reasonable Security Measures

BEST PRACTICES

- Include reasonable security requirements in service provider contracts
- Verify compliance during contracts period

FTC CASE: GMR TRANSCRIPTION

Hired service providers to transcribe sensitive audio files but failed to require reasonable security measures

For example: Encryption

FROM: Start with Security: A Guide for Business, FTC

CyberSecure MY BUSINESS

9. Put Procedures in Place to Keep Security Current and Address Vulnerabilities

BEST PRACTICES

- Update and patch 3rd party software when urgent need and on regular schedule
- Act quickly on credible warnings and ensure risks are addressed

FTC CASE: FANDANGO

Security warning wrongly categorized as customer service request was ignored.

FROM: Start with Security: A Guide for Business, FTC

10. Secure Paper, Physical Media and Devices

BEST PRACTICES

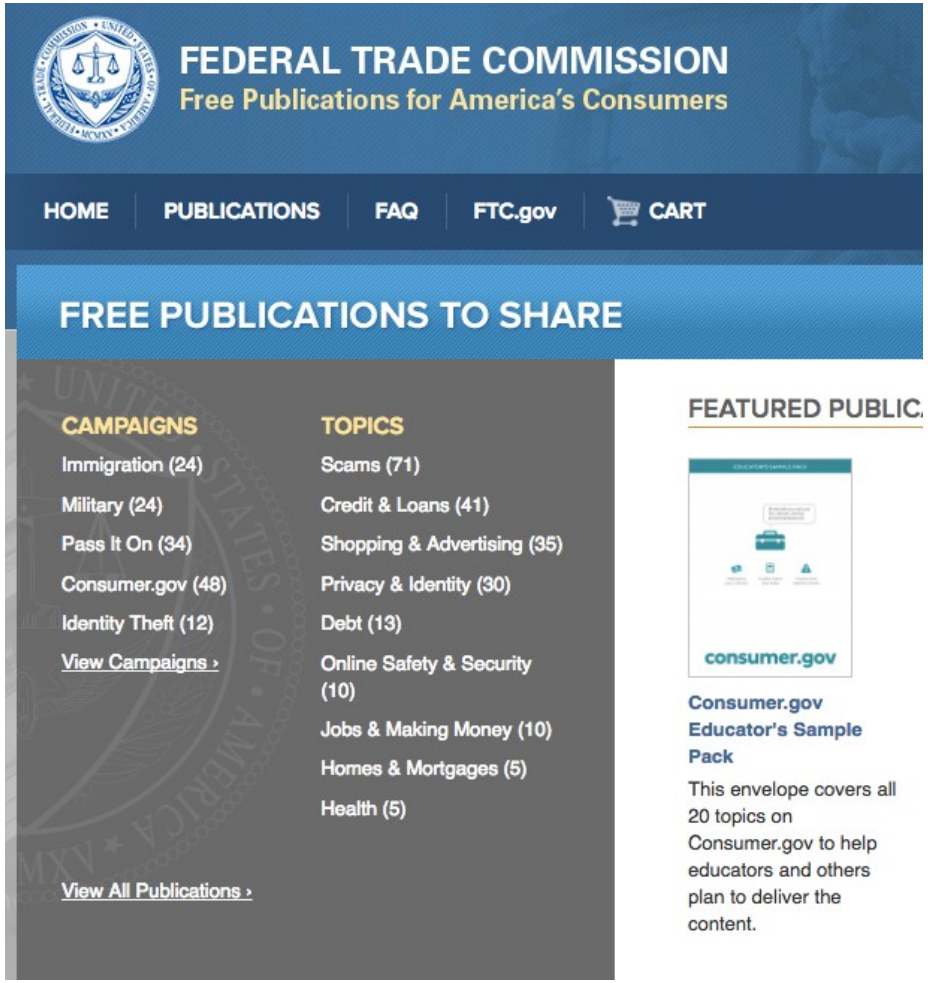
- Protect mobile and storage devices on the move when traveling or commuting
- Secure paper records –lock up sensitive items
- Dispose of sensitive personal data securely – disk drives, printers etc.

FTC CASE: GOAL FINANCIAL

Employee sold surplus hard drives with unencrypted sensitive information of 34,000 customers.

FROM: Start with Security: A Guide for Business, FTC

Federal Trade Commission – *Even More*



FREE PUBLICATIONS TO SHARE

CAMPAIGNS

- Immigration (24)
- Military (24)
- Pass It On (34)
- Consumer.gov (48)
- Identity Theft (12)
- View Campaigns ›

TOPICS

- Scams (71)
- Credit & Loans (41)
- Shopping & Advertising (35)
- Privacy & Identity (30)
- Debt (13)
- Online Safety & Security (10)
- Jobs & Making Money (10)
- Homes & Mortgages (5)
- Health (5)

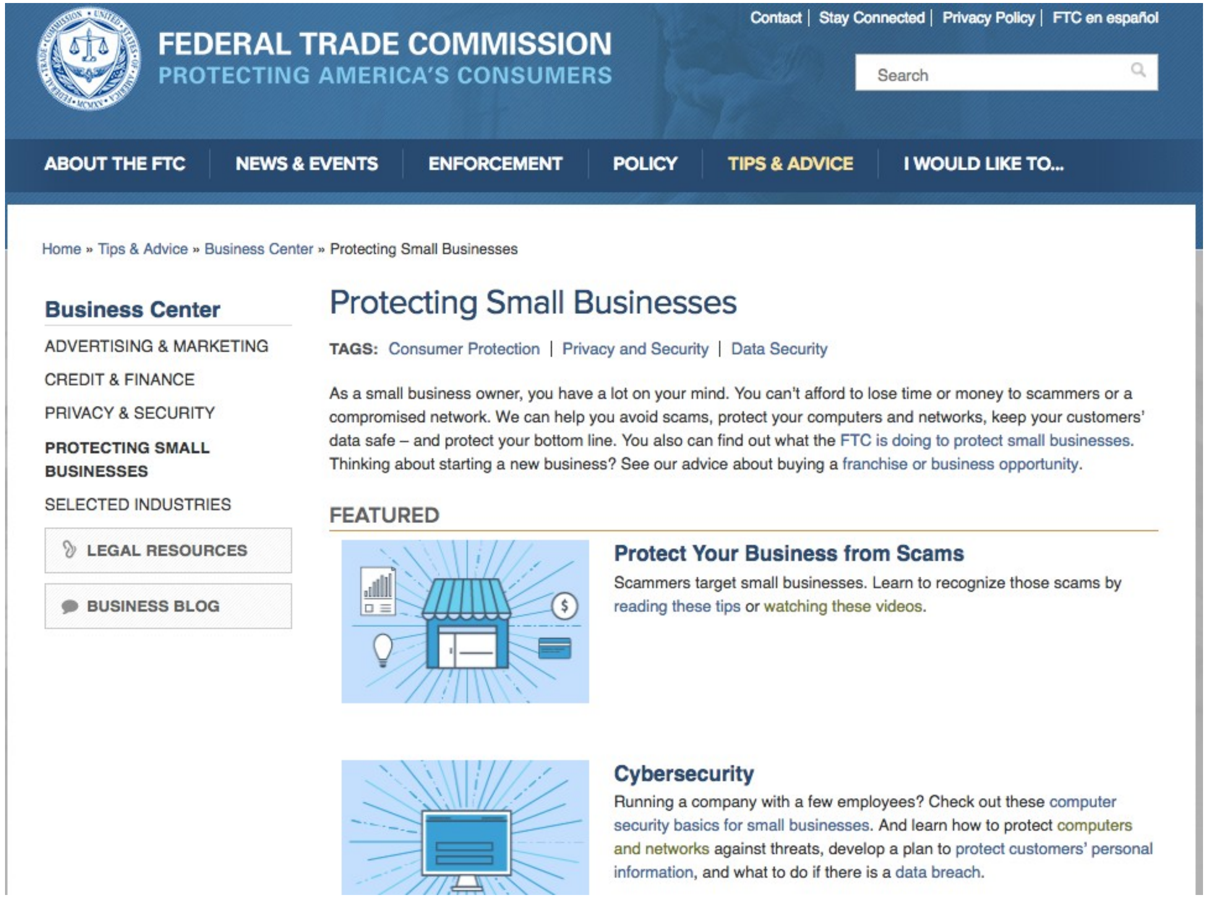
View All Publications ›

FEATURED PUBLIC

Consumer.gov Educator's Sample Pack

This envelope covers all 20 topics on Consumer.gov to help educators and others plan to deliver the content.

Bulkorder.ftc.gov



Home » Tips & Advice » Business Center » Protecting Small Businesses

Business Center

- ADVERTISING & MARKETING
- CREDIT & FINANCE
- PRIVACY & SECURITY
- PROTECTING SMALL BUSINESSES
- SELECTED INDUSTRIES
- LEGAL RESOURCES
- BUSINESS BLOG

Protecting Small Businesses

TAGS: Consumer Protection | Privacy and Security | Data Security

As a small business owner, you have a lot on your mind. You can't afford to lose time or money to scammers or a compromised network. We can help you avoid scams, protect your computers and networks, keep your customers' data safe – and protect your bottom line. You also can find out what the FTC is doing to protect small businesses. Thinking about starting a new business? See our advice about buying a franchise or business opportunity.

FEATURED

Protect Your Business from Scams

Scammers target small businesses. Learn to recognize those scams by reading these tips or watching these videos.

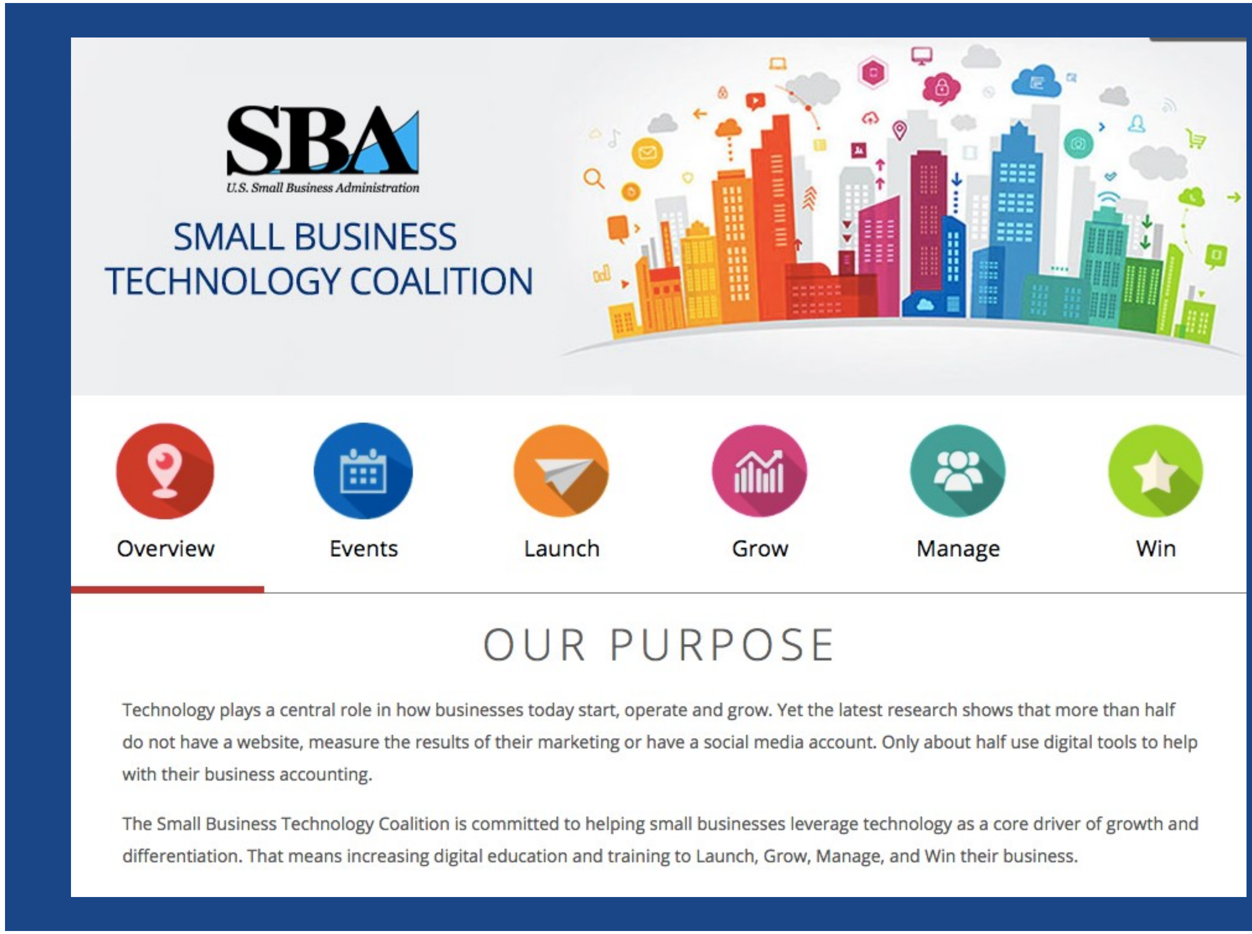
Cybersecurity

Running a company with a few employees? Check out these computer security basics for small businesses. And learn how to protect computers and networks against threats, develop a plan to protect customers' personal information, and what to do if there is a data breach.

Ftc.gov/smallbusiness

CyberSecure MY BUSINESS

U.S. Small Business Administration


SBA
U.S. Small Business Administration
SMALL BUSINESS TECHNOLOGY COALITION
Overview
Events
Launch
Grow
Manage
Win

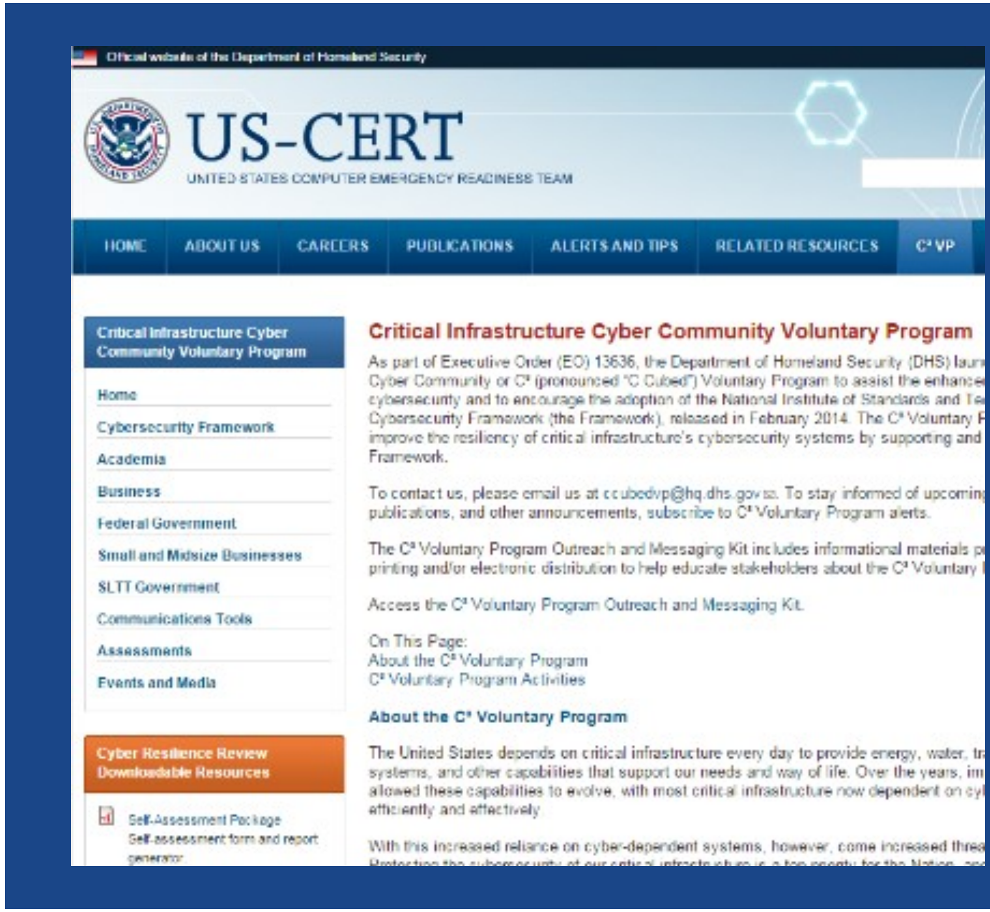
OUR PURPOSE

Technology plays a central role in how businesses today start, operate and grow. Yet the latest research shows that more than half do not have a website, measure the results of their marketing or have a social media account. Only about half use digital tools to help with their business accounting.

The Small Business Technology Coalition is committed to helping small businesses leverage technology as a core driver of growth and differentiation. That means increasing digital education and training to Launch, Grow, Manage, and Win their business.

Committed to helping small businesses leverage technology as a core driver of growth and differentiation. That means increasing digital education and training to Launch, Grow, Manage, and Win their business.

Critical Infrastructure Cyber Community (C^3) Voluntary Program


Official website of the Department of Homeland Security
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
HOME
ABOUT US
CAREERS
PUBLICATIONS
ALERTS AND TIPS
RELATED RESOURCES
C³ VP
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

Critical Infrastructure Cyber Community Voluntary Program

As part of Executive Order (EO) 13636, the Department of Homeland Security (DHS) laun Cyber Community or C^3 (pronounced "C Cubed") Voluntary Program to assist the enhance cybersecurity and to encourage the adoption of the National Institute of Standards and Te Cybersecurity Framework (the Framework), released in February 2014. The C^3 Voluntary P improve the resiliency of critical infrastructure's cybersecurity systems by supporting and Framework.

To contact us, please email us at ccubedvp@hq.dhs.gov. To stay informed of upcomin publications, and other announcements, subscribe to C^3 Voluntary Program alerts.

The C^3 Voluntary Program Outreach and Messaging Kit includes informational materials p printing and/or electronic distribution to help educate stakeholders about the C^3 Voluntary

Access the C^3 Voluntary Program Outreach and Messaging Kit.

On This Page:
About the C^3 Voluntary Program
C^3 Voluntary Program Activities

About the C^3 Voluntary Program

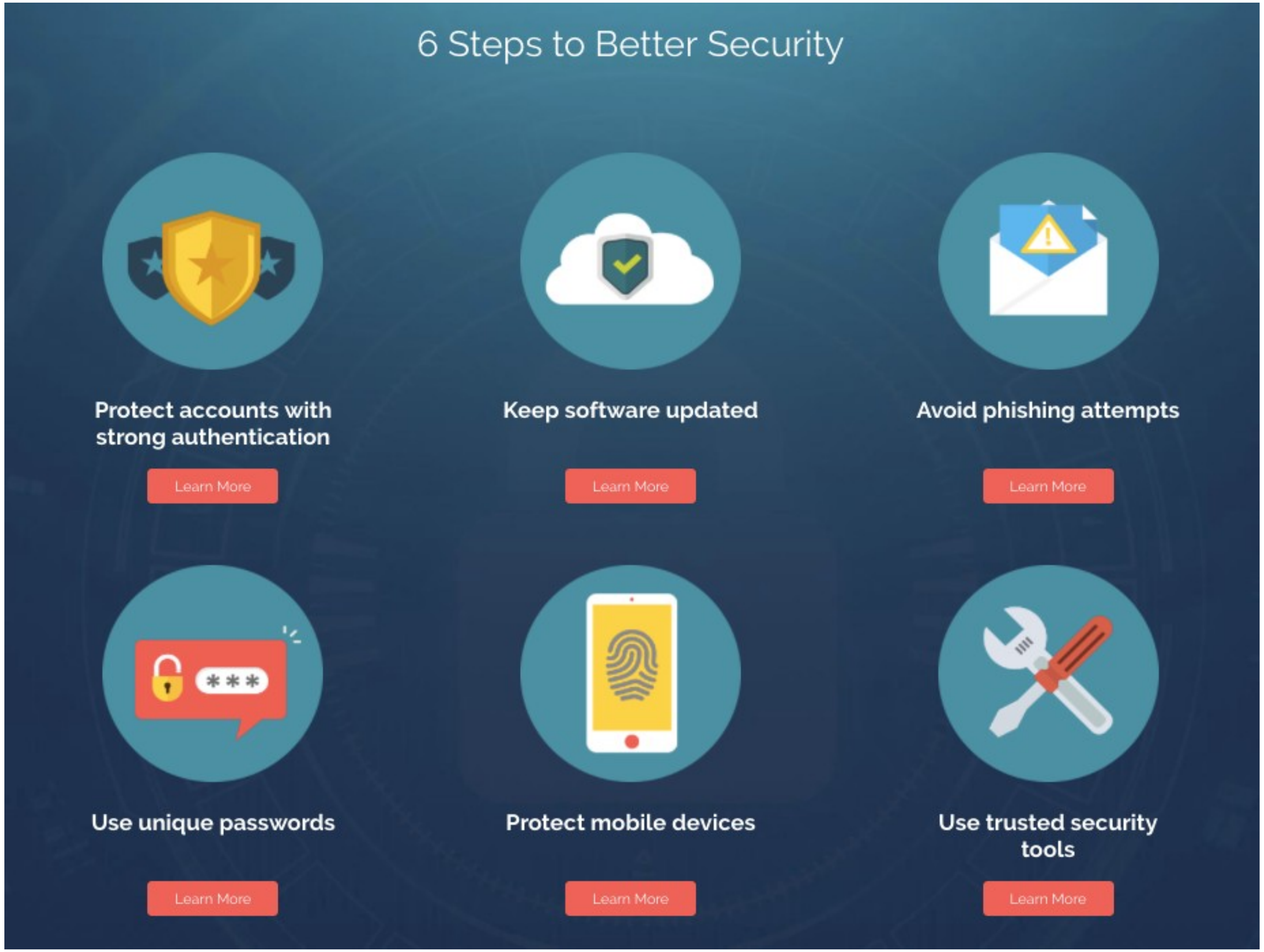
The United States depends on critical infrastructure every day to provide energy, water, tr systems, and other capabilities that support our needs and way of life. Over the years, im allowed these capabilities to evolve, with most critical infrastructure now dependent on cy efficiently and effectively.

With this increased reliance on cyber-dependent systems, however, come increased threa

Self-Assessment Package
Self-assessment form and report generator

- Over 40 no-cost resources currently featured, including the Cyber Resilience Review and the SMB Toolkit
- Pages are organized by stakeholder group, including Small and Midsize Business
- Resources are aligned by Framework Core Function: Identify, Protect, Detect, Respond, and Recover

LockDownYourLogin.Org



6 Steps to Better Security

Protect accounts with strong authentication

Learn More

Keep software updated

Learn More

Avoid phishing attempts

Learn More

Use unique passwords

Learn More

Protect mobile devices

Learn More

Use trusted security tools

Learn More

CyberSecure MY BUSINESS

Goal of 5-Step Approach is Resilience

Know the threats and Identify and Protect your assets

Detect problems and respond quickly and appropriately

Know what recovery looks like and prepare

CyberSecure
MY BUSINESS

PLAN. PROTECT. RESPOND.

Thank You

NATIONAL
CYBERSECURITY
ALLIANCE