Cyber Threats & Prevention

Phishing, Ransomware, BEC, and How to Protect Yourself

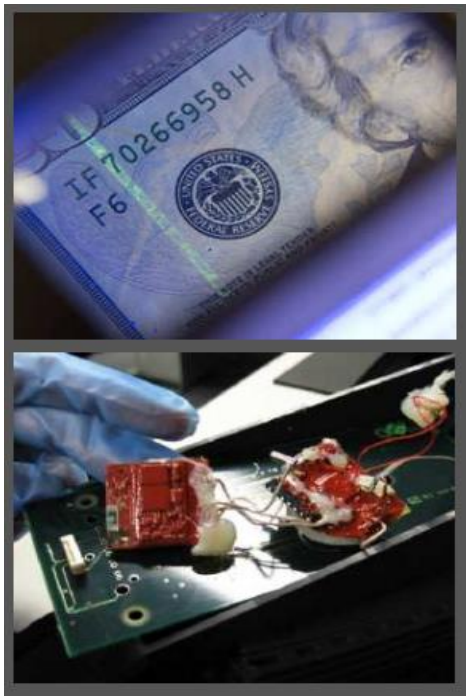
Today's Topics

- US Secret Service and the Cyber Fraud Task Force
  - Current conditions
- Threats
  - Phishing
  - Ransomware
  - Business Email Compromise (BEC)
- Vulnerabilities
  - Weak Passwords
  - Old software
- Protection
  - Best Practices
  - CISA Cyber Hygiene Services

Mission of Secret Service

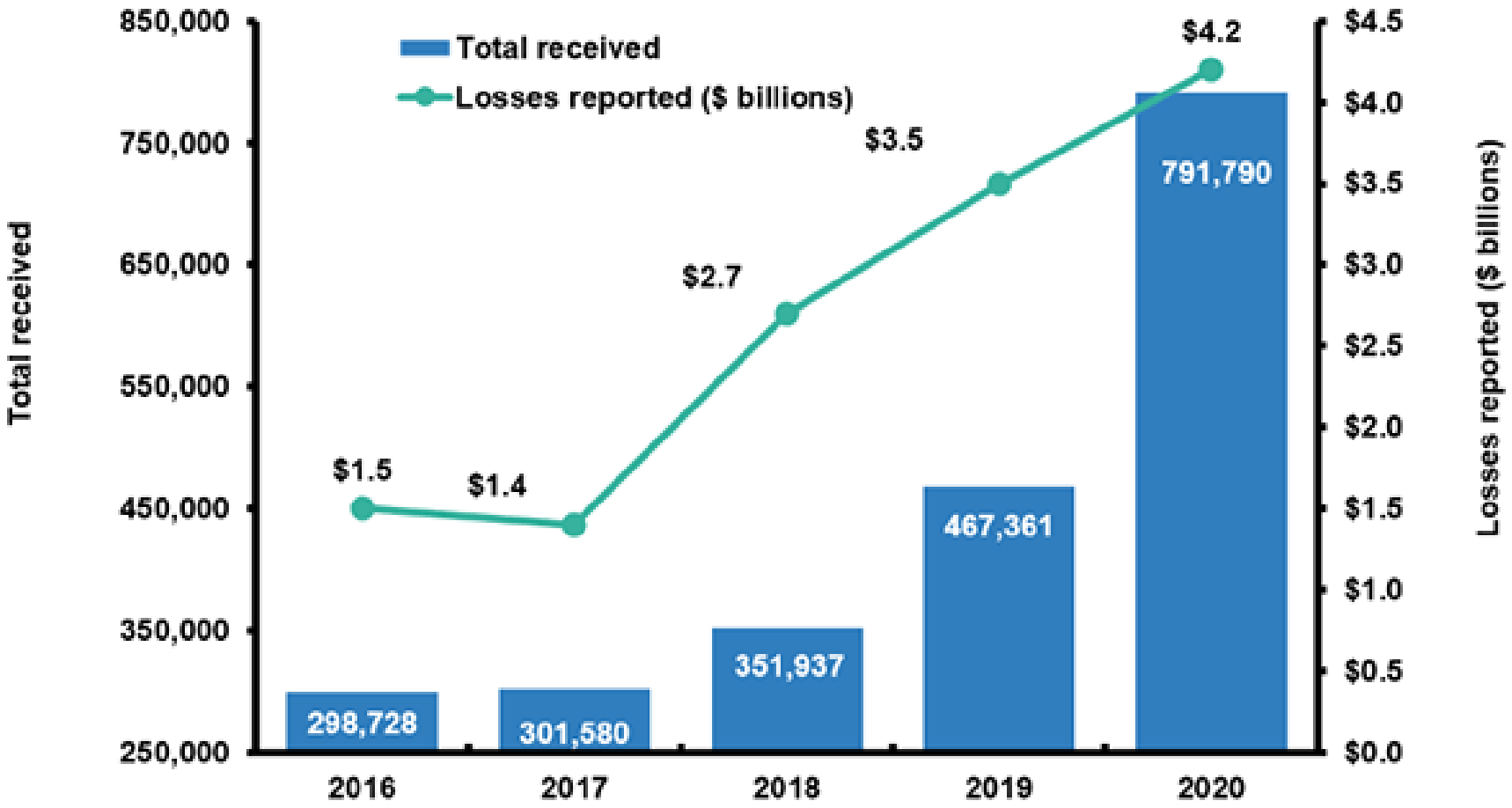
The United States Secret Service is mandated by statute and executive order to carry out two significant missions:

Protection & Investigation



Cyber Fraud Task Force

Fraud Complaints and Losses



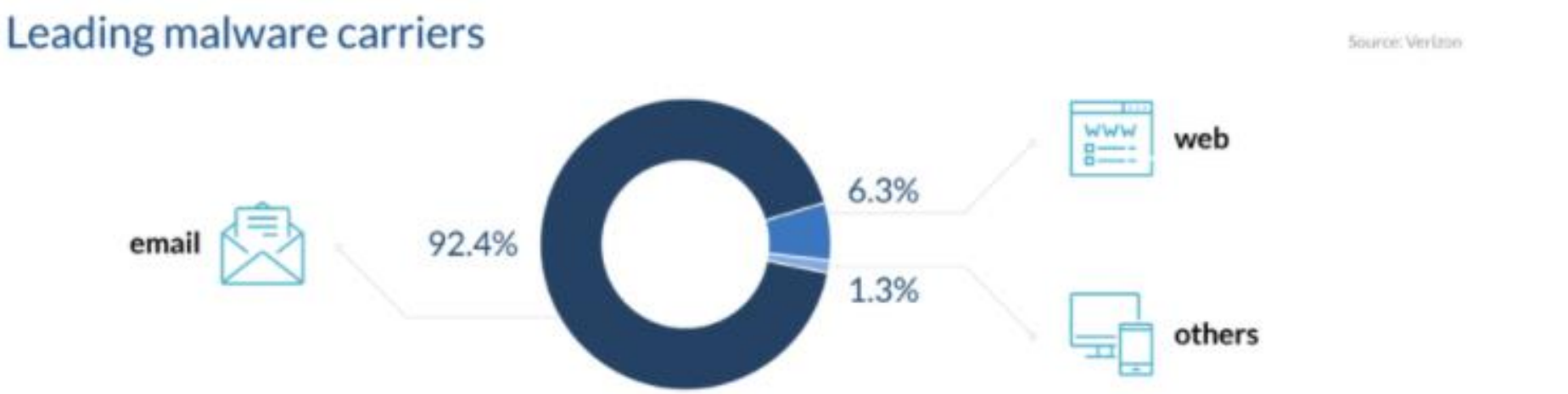
Source: Internet Crime Complaint Center

Phishing Attacks

Phishing Attacks

A type of social engineering where an attacker sends a fraudulent message designed to trick a victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure

Malware Vectors



- 46% of organizations receive emails containing malware. (Verizon, 2020)
- 29% of users will open phishing emails. (Proofpoint, 2020)
- Only 30% of companies test employees awareness of phishing (AT&T)

Types of Phishing Attacks

- Spear – phishing attempts directed at specific companies or individuals.

- Clone – a legitimate and previously delivered email with an attachment is cloned and the attachment is replaced with malicious code.

- Whaling – phishing attacks directed at senior executives and other high profile personnel within an agency or company.

Phishing Characteristics

Messages are often urgent or threatening

Graphics mimic those of the real company

Typically, users are asked to click a link which turns out to be phony

Phishing Examples

NETFLIX

Your Account | Queue | Help

Your Account Has Been Suspended

Dear Netflix,

We are sending this email to let you know that your credit card has been expired. To update your account information, please visit Your Account.

-Your friends at Netflix

ups

Hi <customer>,

This is a follow-up regarding your package delivery:

- Tracking Number: 0p2uYq5RIho

The package contained in the above-mentioned shipment was not accepted at the de
Please contact your local UPS office and provide the printed delivery sticker, included in this email.

Please note that in case of a failure to contact your local UPS office within 21 days the parcel will be returned to sender.

Thanks so much for shipping with UPS.

Get the UPS My Choice app for Facebook

Download the UPS mobile app

amazon

Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

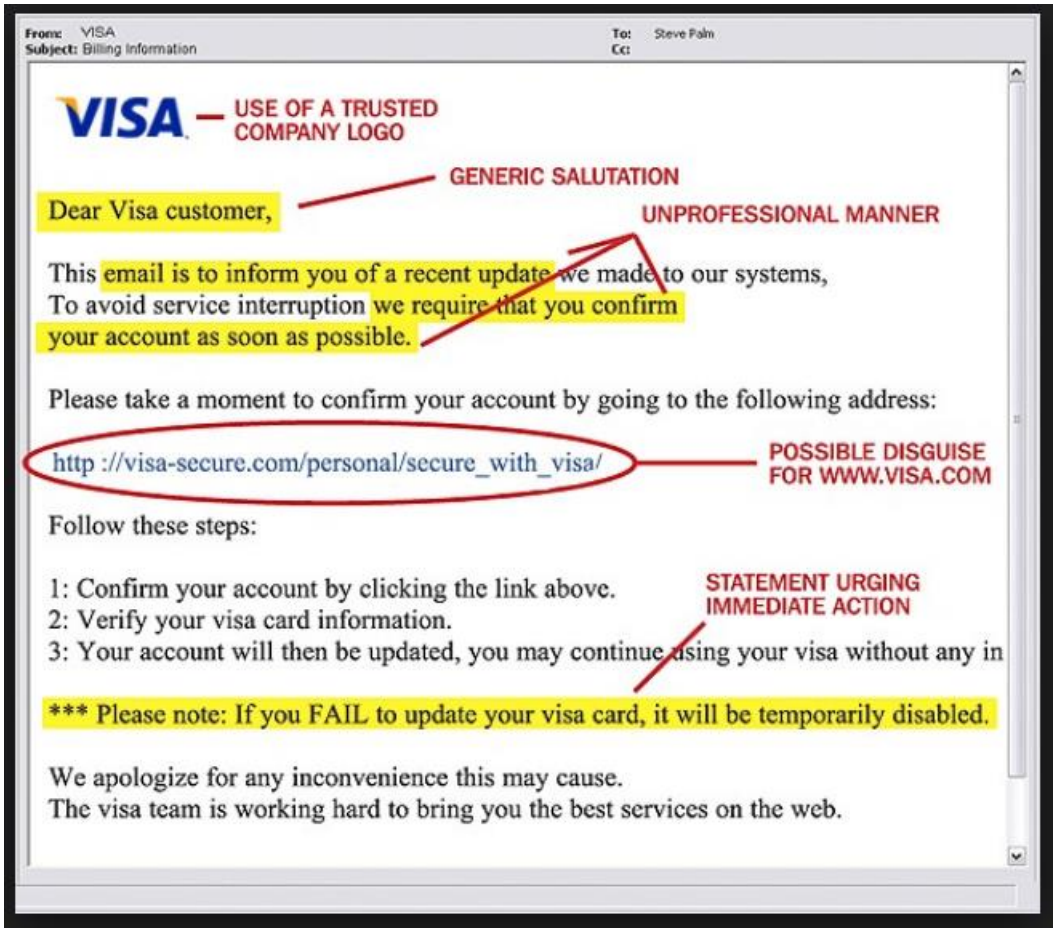
You are required to provide us a valid billing address

Click Here to Update Your Address

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.
Amazon.com
Email ID:

Phishing Example



Combating Phishing

Inspect links before clicking

Combating Phishing

http://www.stealmyinformation.com/
Ctrl+Click to follow link

http://www.in.gov/cyber

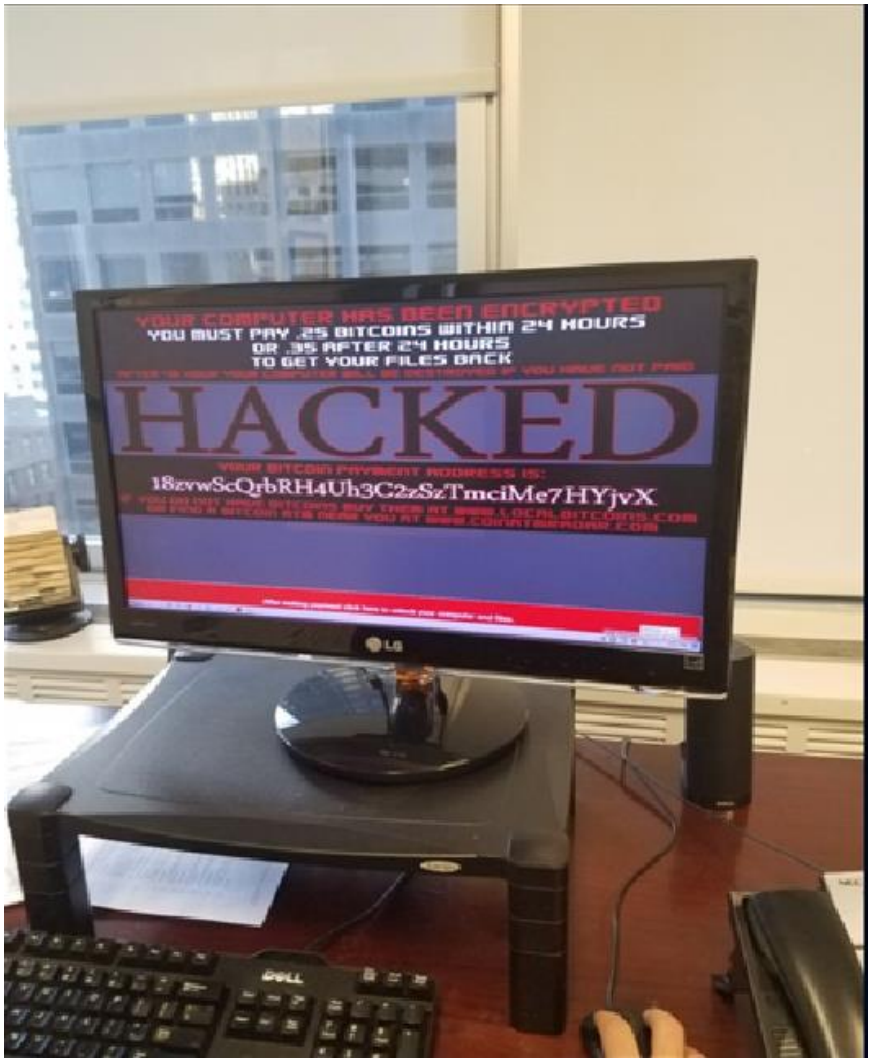
Inspect links before clicking

Ransomware

Ransomware

Malware that employs encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. A ransom is then demanded to provide access or prevent publication.

Ransomware


YOUR COMPUTER HAS BEEN ENCRYPTED
YOU MUST PAY .25 BITCOINS WITHIN 24 HOURS
OR .35 AFTER 24 HOURS
TO GET YOUR FILES BACK
HACKED
YOUR BITCOIN PAYMENT ADDRESS IS:
18zvwScQrbRH4Uh3C2zSzTmciMe7HYjvX

Ransomware


CryptoLocker
Your Personal files are encrypted!
Your personal files encryption produced on this computer: photos, videos, documents, etc. Encryption was produced using a unique public key RSA-2048 generated for this computer.
To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow 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 1.00 bitcoin (~291 USD).
You can easily delete this software, but know that without it, you will never be able to get your original files back.
Disable your antivirus to prevent the removal of this software.
For more information on how to buy and send bitcoins, click "Pay with Bitcoin"
To open a list of encoded files, click "Show files"
Do not delete this list, it will be used for decryption. And do not move your files.
Private key will be destroyed on
1/6/2015 1:11:47 PM
Time left
71:52:21
Checking wallet..
Received: 0.00 BTC
Show files
Pay with Bitcoin

What if I'm hit with ransomware?

1. **Determine which systems were impacted, and immediately isolate them.**

- If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
- Isolate systems in a coordinated manner. Not doing so could cause actors to move laterally to preserve their access—already a common tactic—or deploy ransomware widely prior to networks being taken offline.

2. If you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection. This will destroy some evidence

3. Identify the ransomware: **NoMoreRansom.org**

- The site has a suite of tools to help you free your data, including the Crypto Sheriff tool: Just upload one of your encrypted files and it will scan to find a match.

4. Triage impacted systems for restoration and recovery.

5. Once ransomware has been removed, change all system passwords

(www.stopransomware.gov)

To Pay or Not to Pay

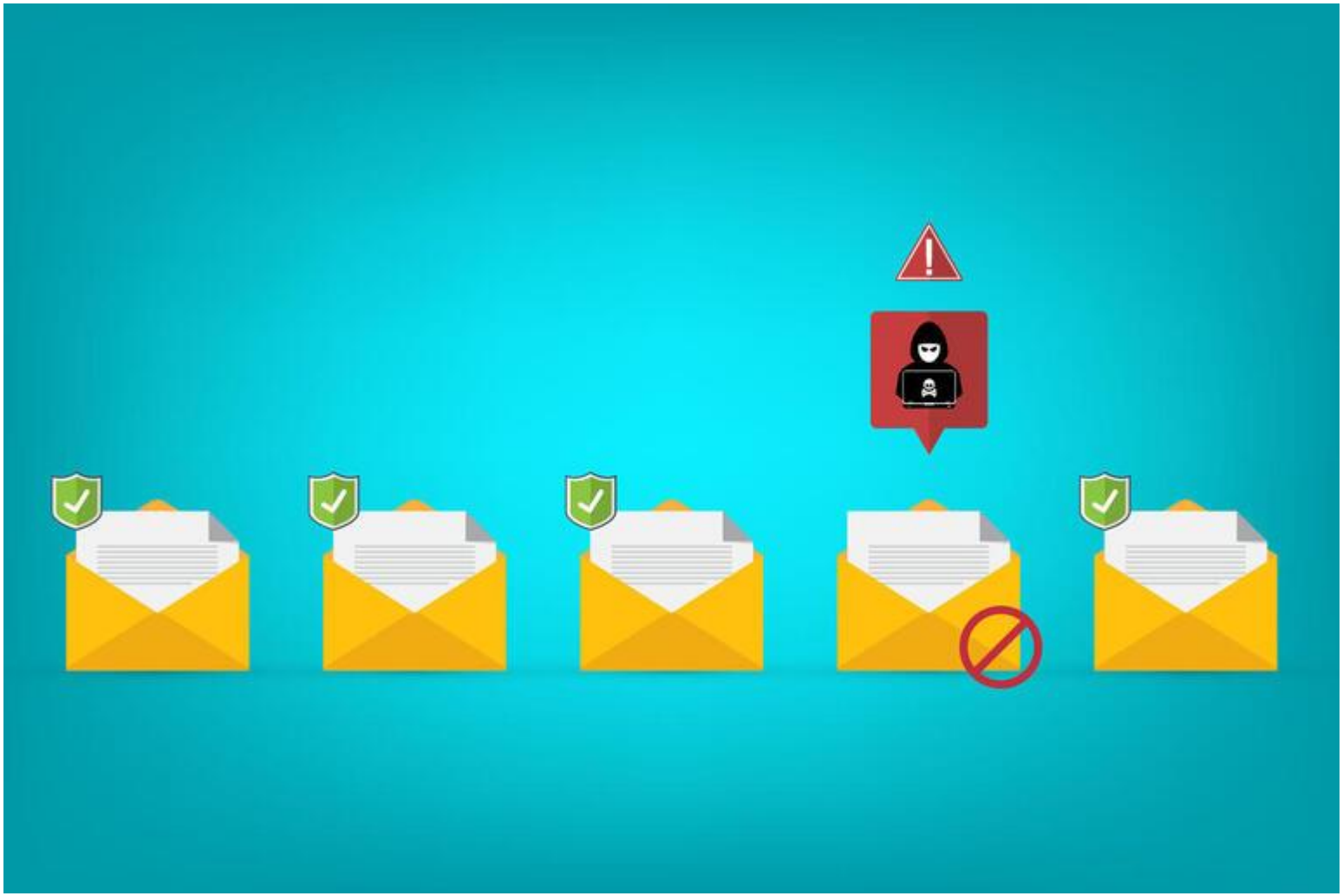
- **US Gov't does NOT encourage paying a ransom**
  - You may never get a decryption key.
  - You could get repeated ransom demands.
  - You may receive a decryption key that works—*kind of.*
  - You may be painting a target on your back.
  - Even if everything somehow ends up fine, you're still funding criminal activity.
- 70% of surveyed businesses paid the ransom (Symantec / IBM-X)
- The average ransom payment decreased 34% to **$154,108** from $233,817 in Q3 of 2020. The dramatic reduction was attributed to more victims of data exfiltration attacks saying "ENOUGH" and choosing not to pay. (Coveware, 2020)

Protecting yourself from ransomware

- **Backup network servers.** Perform frequent backups of the system and other important files, and verify the backups regularly.
- **Store backups separately.** Best practice is to store backups on a separate device that cannot be accessed from a network, such as on an external hard drive.
- **Train organization.** Organizations should ensure that they provide cybersecurity awareness training to their personnel. Ideally, organizations will have regular, mandatory cybersecurity awareness training, and test their personnel with phishing assessments that simulate real-world phishing emails.

www.cisa.gov

Business Email Compromise (BEC)



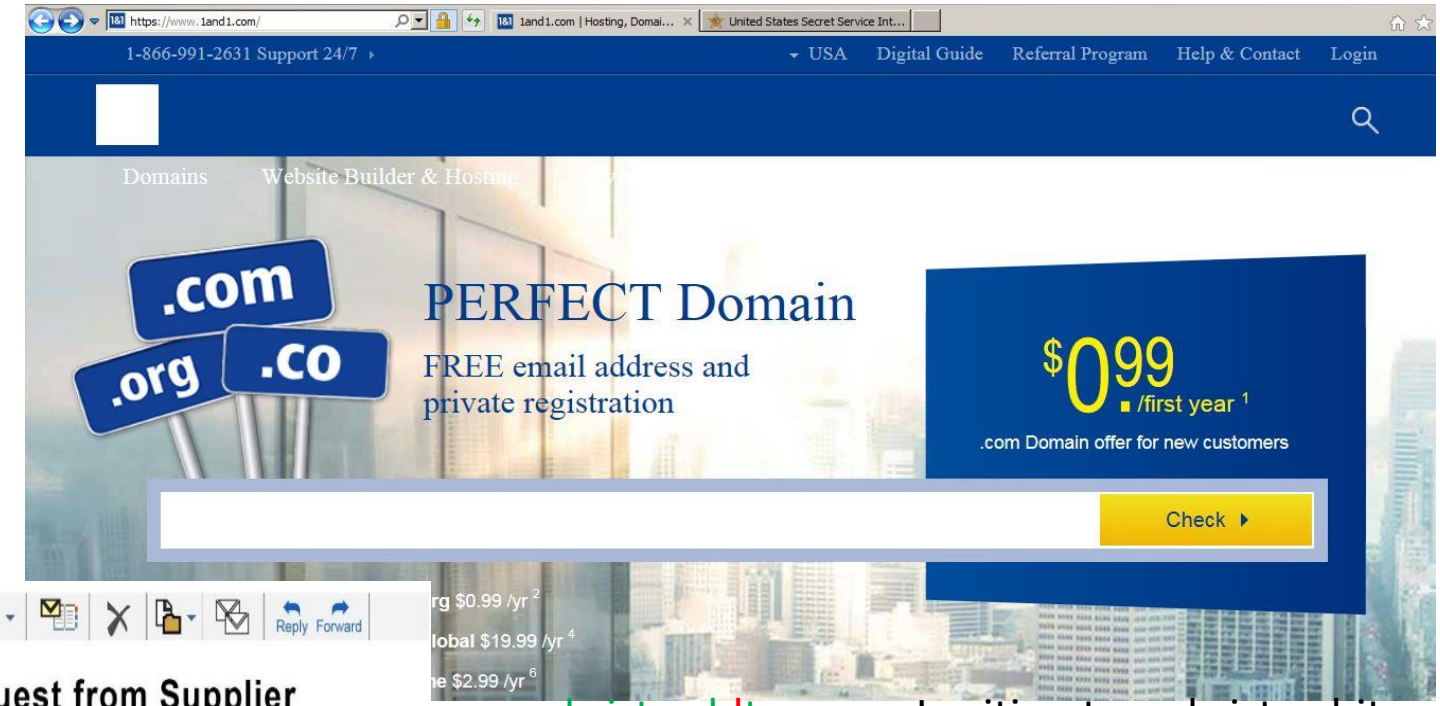
Business Email Compromise (BEC)

A fraud scheme targeting businesses that regularly perform wire transfer payments.

The scam is carried out by compromising legitimate e-mail accounts.

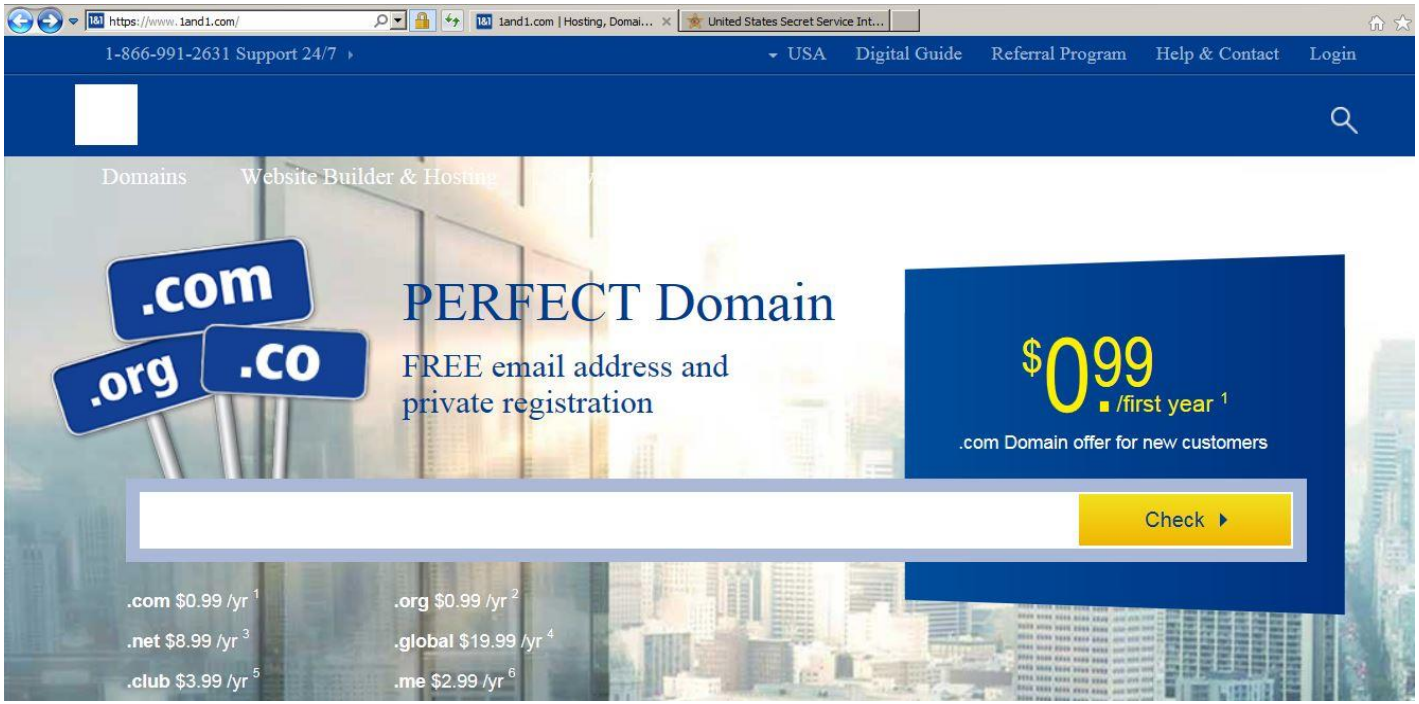
Once compromised, a fraudulent email is sent directing victims to unknowingly conduct unauthorized transfers of funds.

Spoofed Emails and Domains



christywhlte.com Legitimate – christywhite.com
colurnbuszoo.org - Legitimate – columbuszoo.org
nciiinc.com - Legitimate – nciinc.com
rockwellcoliins.com- Legitimate – rockwellcollins.com
turkeyhiil.com - Legitimate – turkeyhill.com
arttherapystudlo.org - Legitimate – arttherapystudio.org
atlanticairnports.com - Legitimate – atlanticaimports.com
decks-dockss.com - Legitimate – decks-docks.com

Spoofed Emails and Domains



lrees@indianapolis.bank

lrees@indiana.bank

Lrees@indiana.bank

Lrees@indiiana.bank

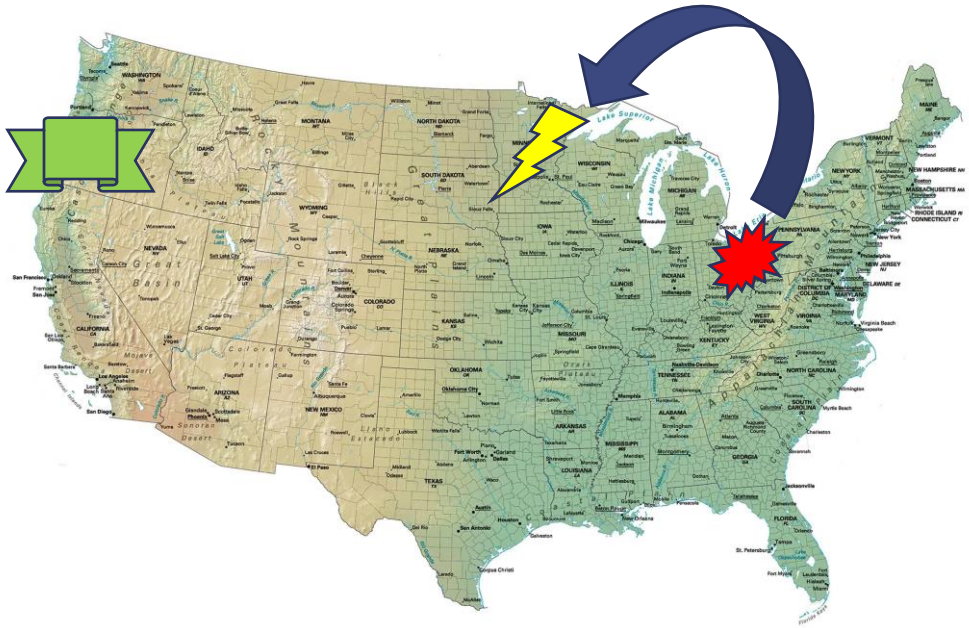
BEC Case Study

There is a network breach at an Ohio-based company and the perpetrator trolls Accounts Payable .

An LLC, which matches name of an Ohio-based company, is established in Oregon.

Perpetrator sees upcoming bill; shows a $1+ million bill due for a Minnesota-base company.

Using an email altered by one letter, perpetrator sends the MN-based company a bill from the OH-based company, with new wiring instructions



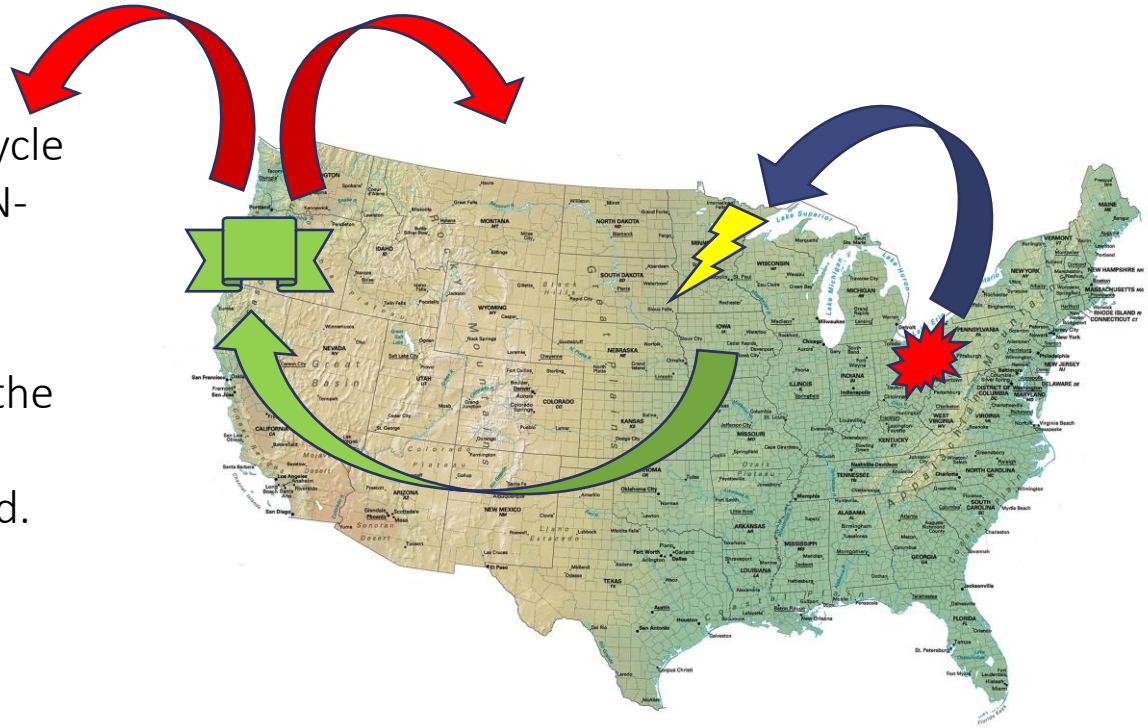
BEC Case Study

The Minnesota-based company wires $1+ million to Oregon, not Ohio.

The OH-based company's billing cycle eventually fails due to result in MN-based company's payment.

The OH-based company contacts the MN-based company, asking for payment and the BEC is discovered.

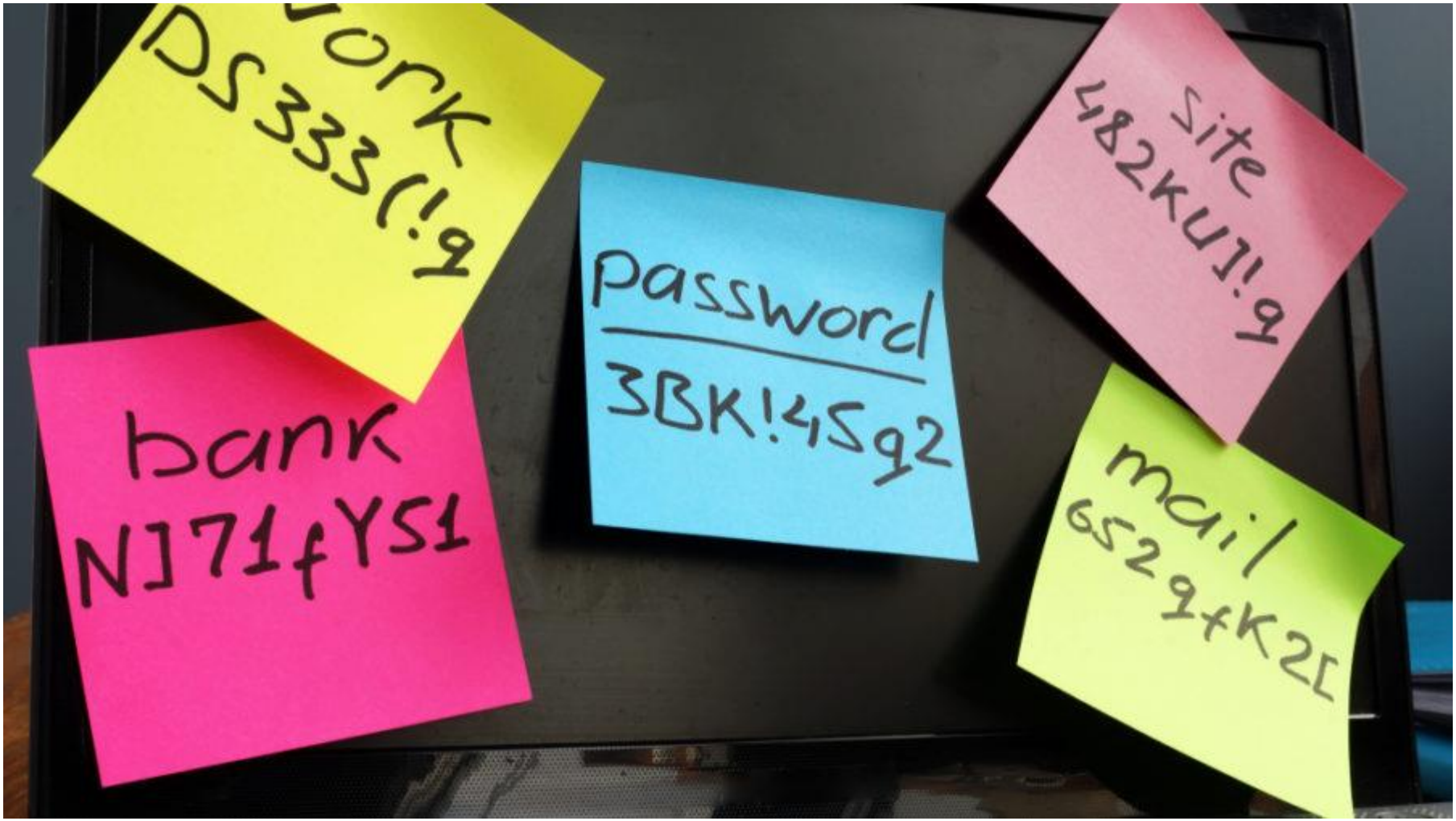
Of the three banks involved in the BEC, only one still had any funds. Less than 20% of the originally wired funds are seized and returned to the victim



BEC: Notification is CRUCIAL

- Domestic Wires: We can send U.S. banks a freeze request and perform an administrative seizure (up to $500K)
- International Wires: If reported within 72 hours, it could be possible to recover funds by locating and freezing accounts before funds are transferred overseas (via Financial Fraud Kill Chain)

Passwords



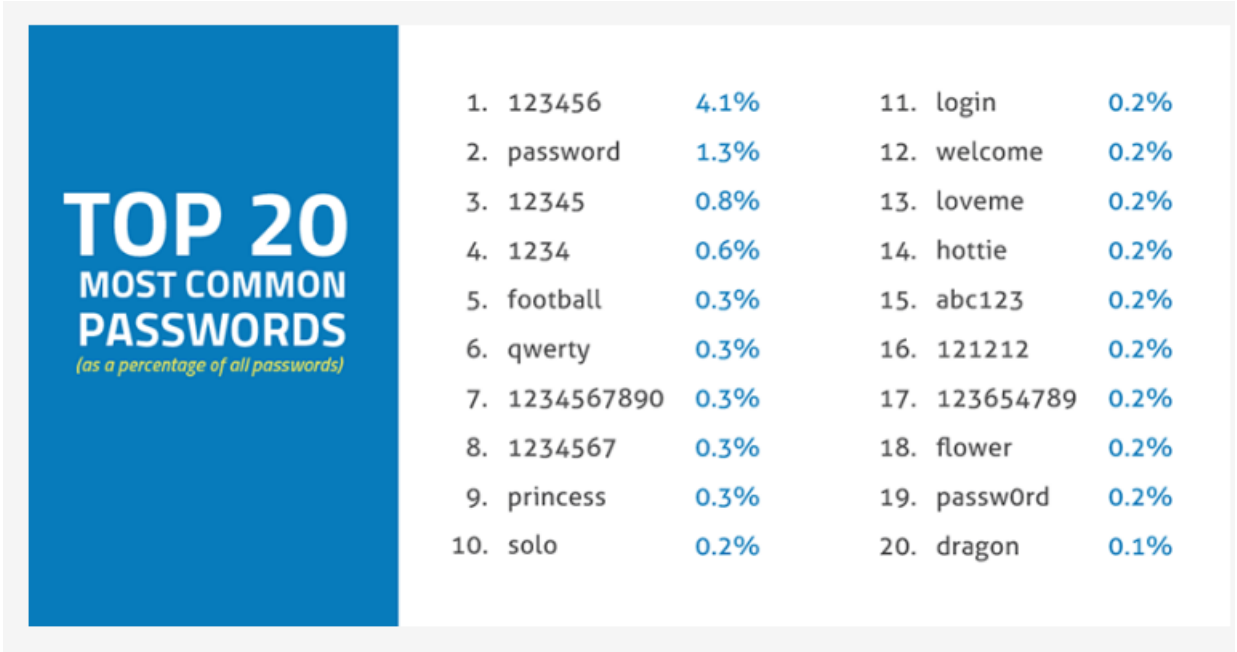
Default Passwords

All it takes is a simple search to identify the default password of any device or software you use within your organization

	2Wire, Inc.	360 Systems
3COM	3M	Accelerated Networks
ACCTON	Acer	Actiontec
Adaptec	ADC Kentrox	AdComplete.com
AddPac Technology	Adobe	ADT
Adtech	Adtran	Advanced Integration

Weak Passwords

A study of over 11 million passwords found that the 20 most popular passwords account for 10.3% of all logins. In fact, on average, if you just tried “1234”, “12345”, or “123456”, you could log into about 5.5% of the accounts in the study. Add the word “password” as a password and you’ve now covered 6.8% of all passwords in use.



Two ways to create a password

1. Create and use a “passphrase”

2. Randomly generated

There’s an App for that.

Making a strong password

1. Think of a meaningful sentence.

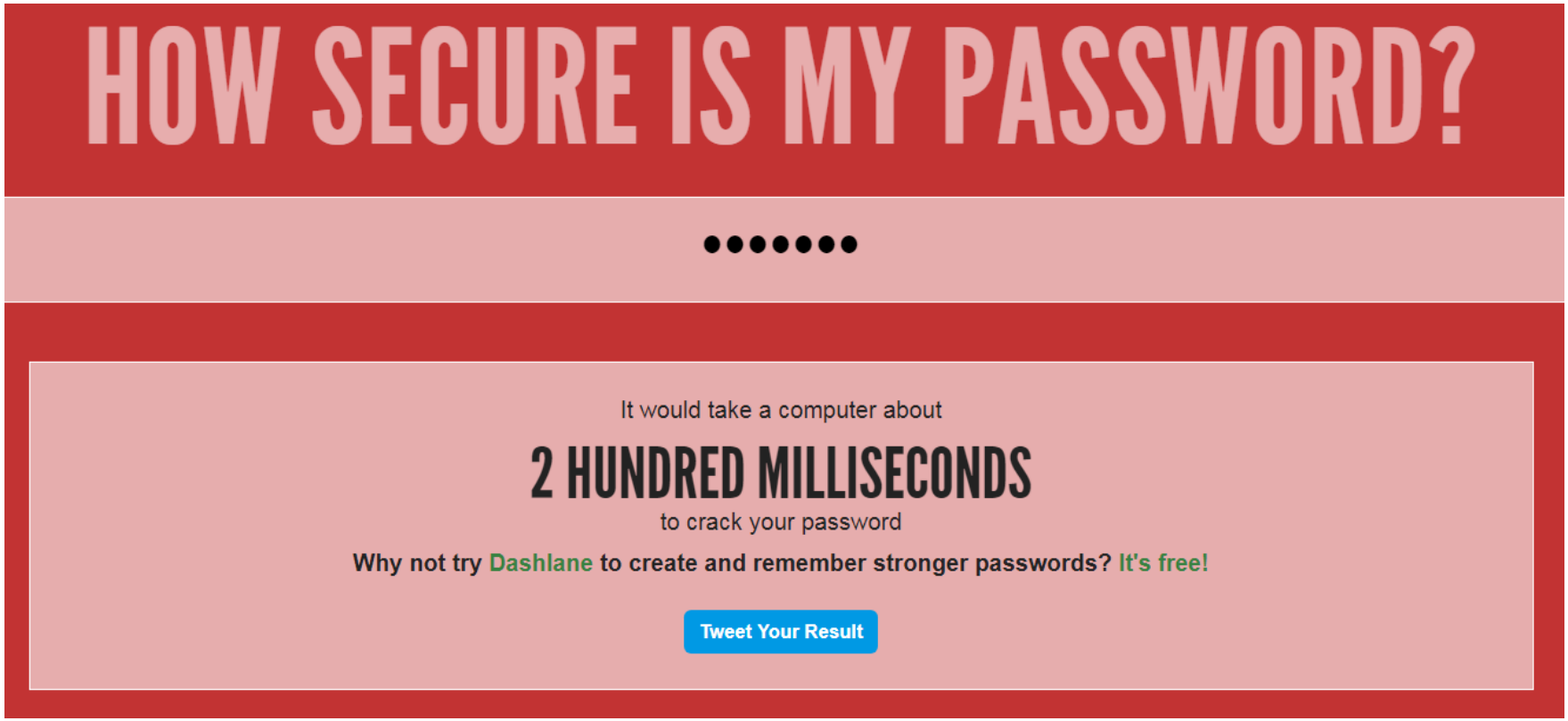
“I’m at the Indiana Bankers Association Conference”

Making a strong password

2. Take the first letter of each word.

“I’m at the Indiana Bankers Association Conference”

iatibac



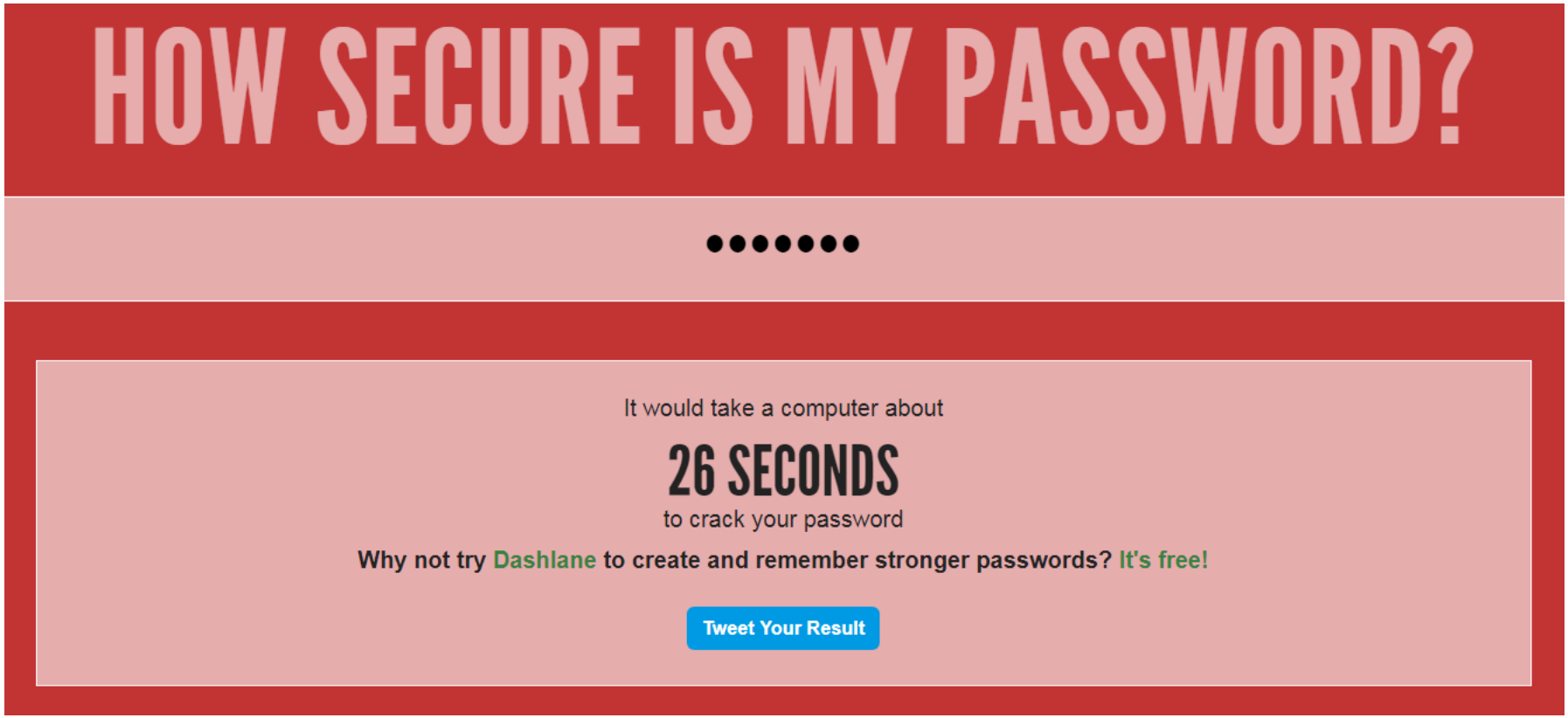
howsecureismypassword.net

Making a strong password

3. Create a mixture of uppercase and lowercase letters.

IatIBAC

IatIBAC

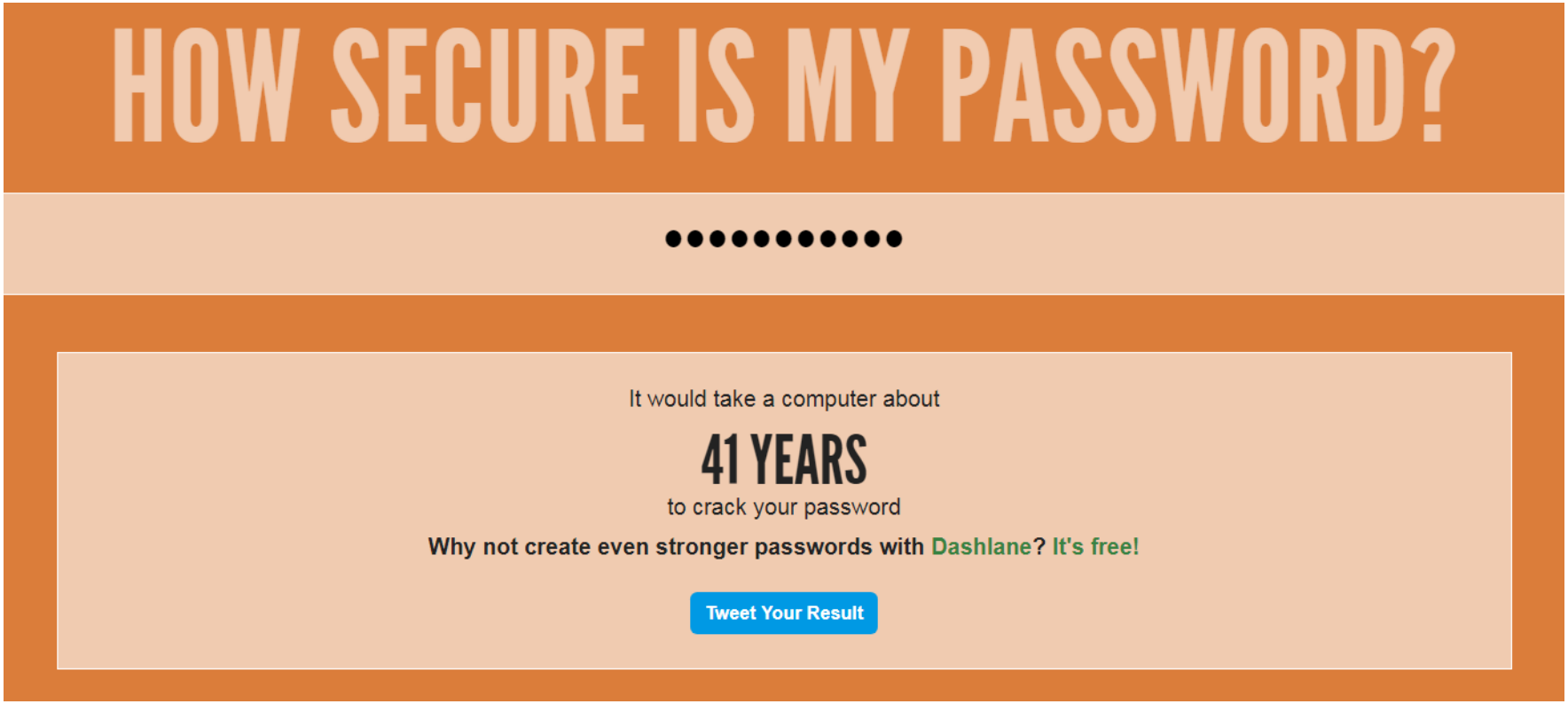


howsecureismypassword.net

Making a strong password

4. Add a number

latIBAC2021



howsecureismypassword.net

Making a strong password

5. Add punctuation

I@tIBAC2021!

I@tIBAC2021!

howsecureismypassword.net

I'm@theIndianaBankersAssociationConference2021!

New Site? New password!

Don’t let a compromise of one site make you vulnerable across the entire internet

Best Practices

Best Practices

- Use strong random passwords (10+ characters, change often, do not use the same password for multiple sites).
- Use two factor authentication when available
- Wired vs wireless (VPN) vs cellular network
- Independently verify all financial requests
- Update antivirus & patches automatically
- Back up your data offline
- HTTPS

How to Protect Yourself

- Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.

- Don’t click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company’s phone number on your own (don’t use the one a potential scammer is providing), and call the company to ask if the request is legitimate.

- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.

- Be careful what you download. Never open an email attachment from someone you don't know, and be wary of email attachments forwarded to you.

CISA Cyber Hygiene Service

Vulnerability Scanning:
Evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

Web Application Scanning:
Evaluates known and discovered publicly-accessible websites for potential bugs and weak configuration to provide recommendations for mitigating web application security risks.

Phishing Campaign Assessment:
Provides an opportunity for determining the potential susceptibility of personnel to phishing attacks. This is a practical exercise intended to support and measure the effectiveness of security awareness training.

Remote Penetration Test:
Simulates the tactics and techniques of real-world adversaries to identify and validate exploitable pathways. This service is ideal for testing perimeter defenses, the security of externally-available applications, and the potential for exploitation of open source information.

https://www.cisa.gov/cyber-hygiene-services

Contact and Resources

Secret Service – Indianapolis
317-635-6420
ind-cftf@usss.dhs.gov

www.stopransomware.gov - CISA Ransomware Info

www.cisa.gov/cyber-hygiene-services

NoMoreRansom.org - ID Ransomware