Agenda

- Threats
  - Cyber Crime Statistics
  - Ransomware
  - BEC/CATO
  - Social Engineering
    - Phishing, Vishing, Smishing, Impersonation
- Prevention
  - NIST Small Business top 20 controls
  - Protect data with encryption, including email
  - Education
  - Remote workforce controls
  - Password Manager/Vault
  - MFA
- Response
  - Cyber Insurance
  - Incident Response Planning

Eye Opening Statistics!

- 95% of cybersecurity breaches are due to human error
- There is a hacker attack every 11 seconds
- Data Breach Investigations Report found that 94% of malware was delivered by email.
- 95% of all cyber attacks use social engineering tactics.
- 93% of company networks can be penetrated by cybercriminals. (betanews.com)

You are of Value to a Hacker

- **Customer Information:** social security numbers, bank account numbers, birthdates, addresses, and contact information
- **Employee Information:** social security numbers, bank account numbers, birthdates, addresses, and contact information
- **Sensitive Corporate Information:** trade secrets, software licenses
- **Email Accounts:** can be compromised and used to send more phishing emails or initiate email fraud attacks
- **Social Media Accounts:** can be compromised to spread false information or defamatory statements
- **Computer Assets:** can be used by hackers to host their information, serve as pivot-points for other attacks, or used to attack (DDos) other computers or networks

Data Breaches?

- **7 Most Common Causes of Data Breach**
  - Weak and Stolen Credentials, a.k.a. Passwords
  - Back Doors, Application Vulnerabilities
  - Malware
  - Social Engineering
  - Too Many Permissions
  - Insider Threats
  - Improper Configuration and User Error

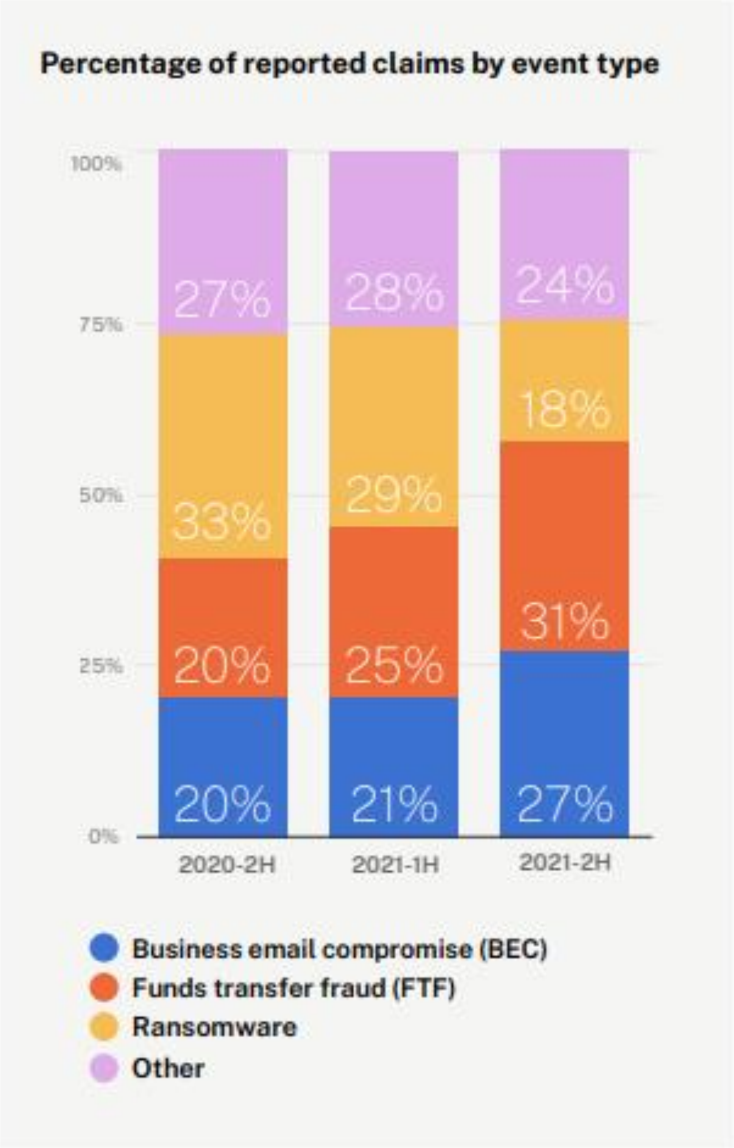
Is There Apathy for Cybersecurity?

- "We don't have anything of value; why would someone want to hack us?"
- "We're too small of a company for a hacker to target."
- "We're in a small, rural area; no one knows who we are."
- "IT will take care of it."
- "We've got a firewall, so we're protected."
- "We trust our people not to fall for scams."
- "We've got insurance; we're covered."

I'M NOT A TARGET

No business is immune to cybercrimes!

Fraudulent Event Types



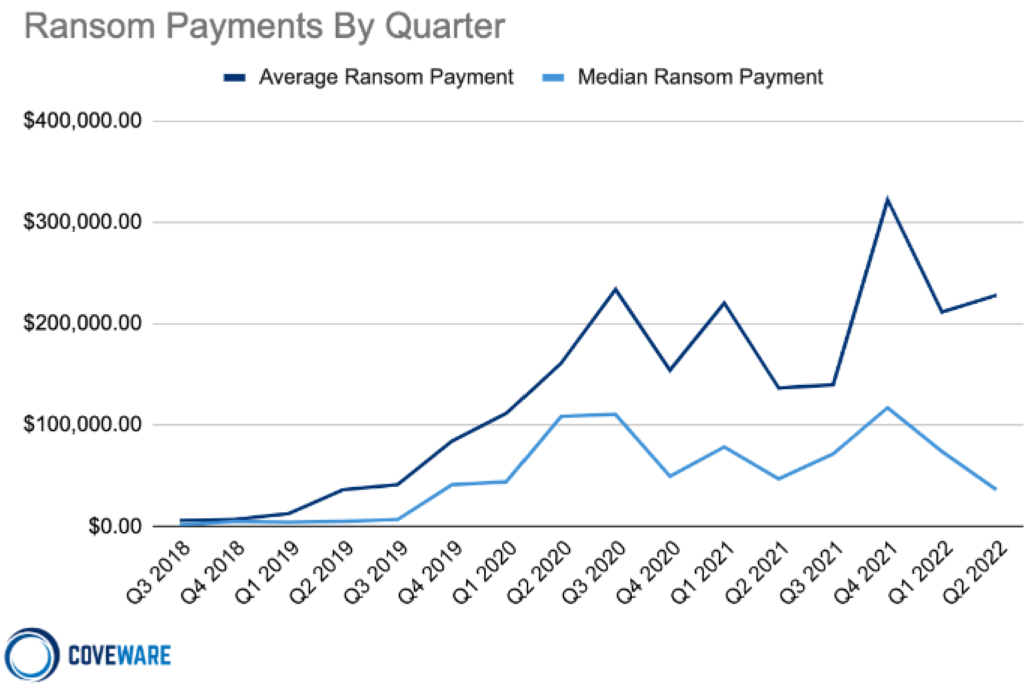
Coalition

What is Ransomware?

- Ransomware is a type of malicious software designed to block access to a computer system or mobile device until a sum of money is paid.
- Ransomware is also referred to "Cyber Extortion".
- Two types of Ransomware:
  - Locker - ransomware denies access to the computer or device.
  - Crypto - ransomware prevents access to files or data.
- Ransomware is often spread through phishing emails that contain malicious attachments or when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge.

Ransomware Payments & Downtime

$228,125 average in Q2 2022 - 8% increase from Q1; $36,360 median (-51%)

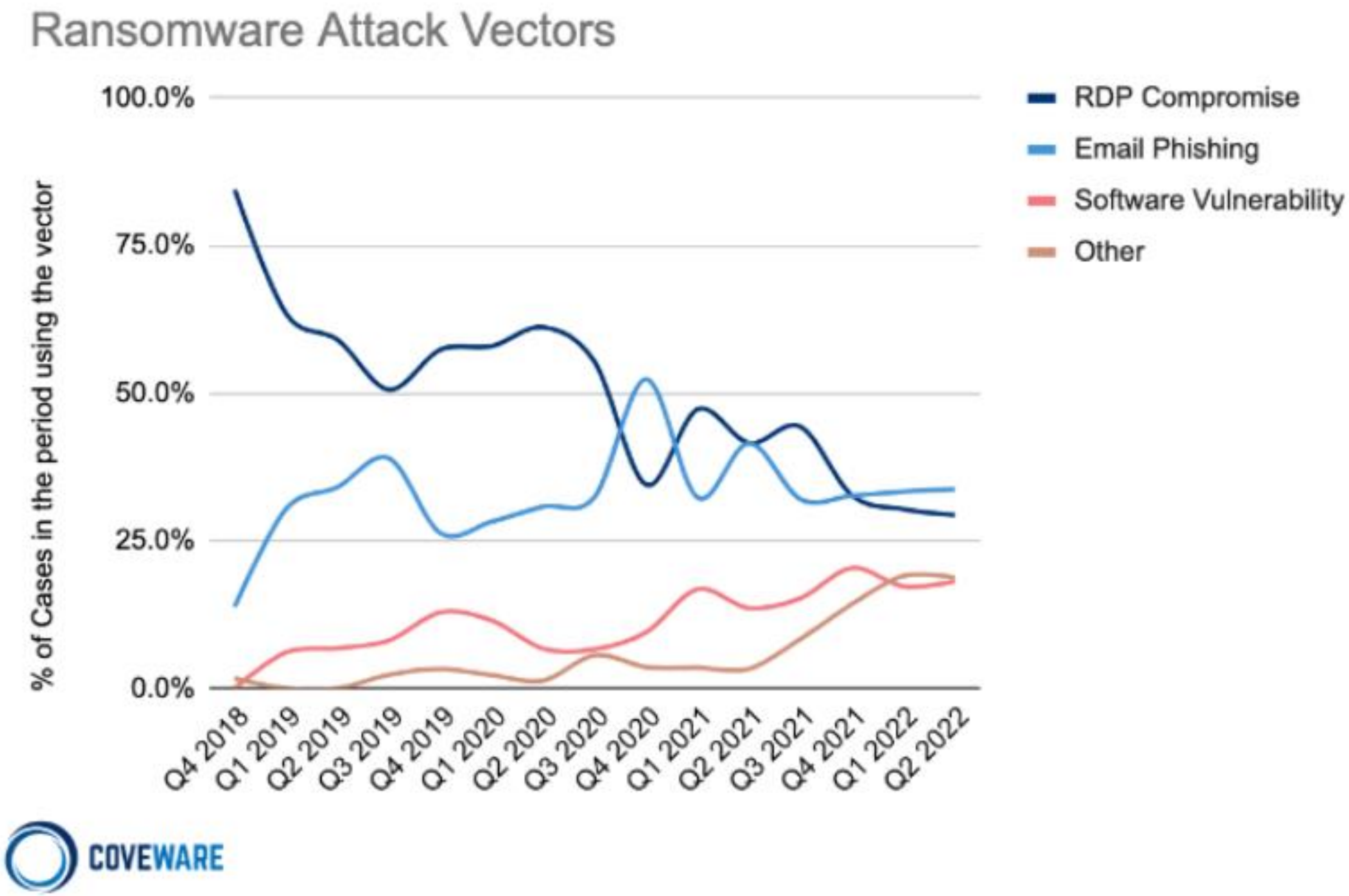


Average downtime = 24 days (-8% from Q1 2022)

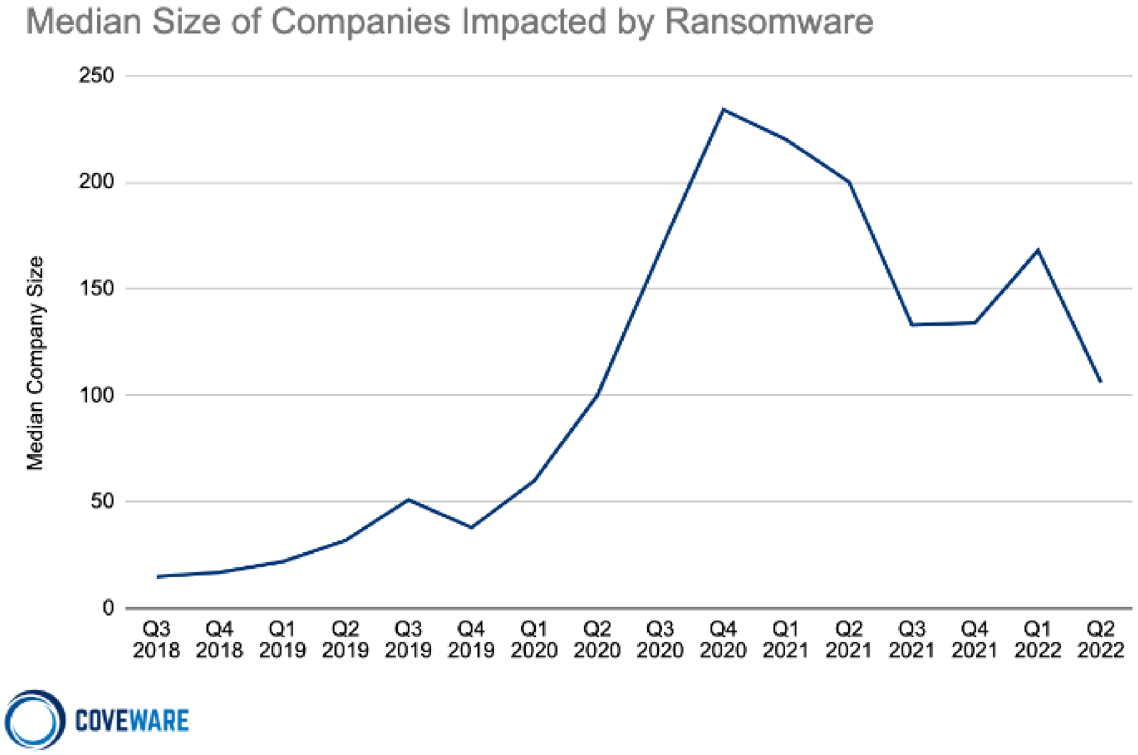
https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

© SBS CyberSecurity, LLC

Ransomware Attack Vectors



Ransomware Trends



86% of Ransomware attacks in Q2 involved data exfiltration

107 =Median # of Employees of Ransomware victims (81% - less than 1000)

https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

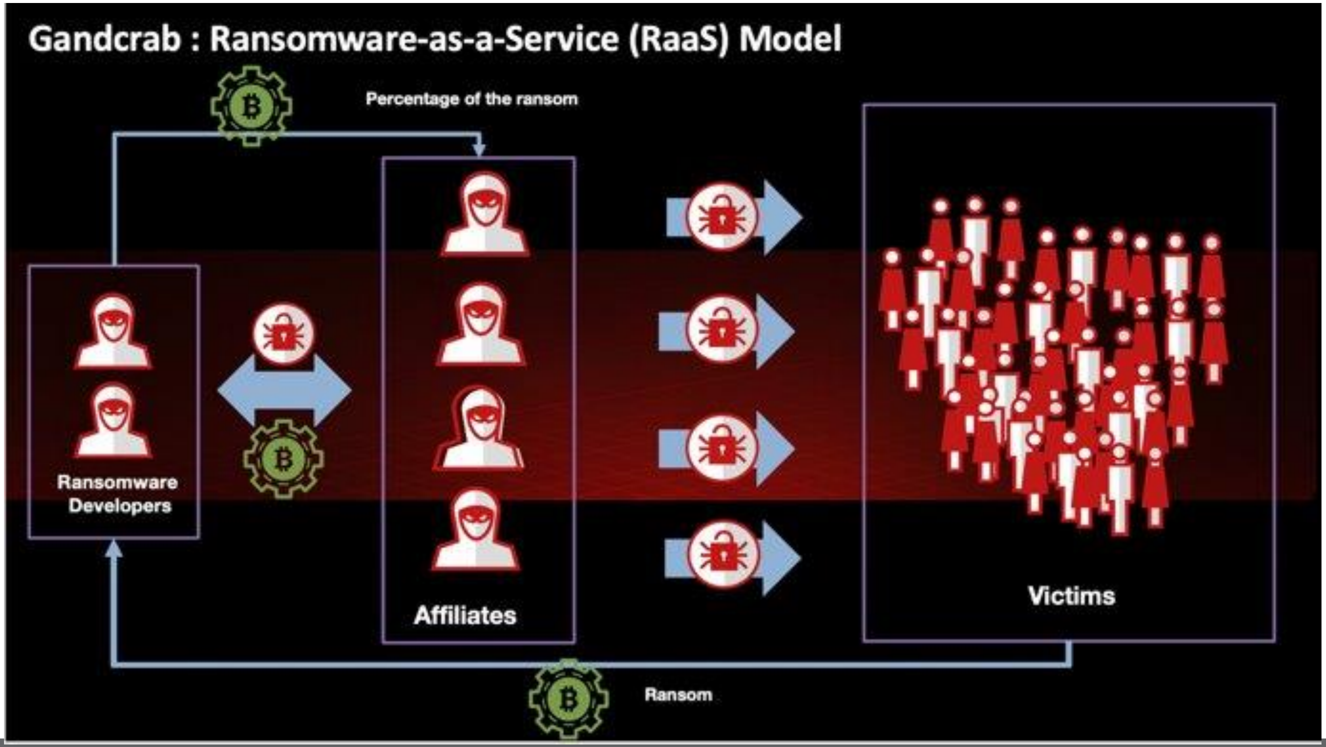
© SBS CyberSecurity, LLC

Ransomware Statistics

- Q2 2022 – Average downtime, 24 days. (Coveware)
- **46%** of enterprise ransomware victims **paid the ransom** in Q1 2022. However, **only 66% were able to fully recover their data. (**Coveware)
- Full cost of **remediation** (getting back to business operations) increases to **$1.85M on average**
- Remember:
  - Paying the ransom doesn't guarantee getting your data back
  - Getting decryption codes doesn't guarantee you'll get your data back
  - You still have to restore, test, and capture manual input from the downtime
- 37 percent of respondents' organizations were affected by ransomware attacks in the last year. (Sophos)
- Cyber Insurance pays 94% or time if it includes ransomware coverage
- In 2022, approximately 71% of all ransomware attacks were successful

Ransomware-as-a-Service

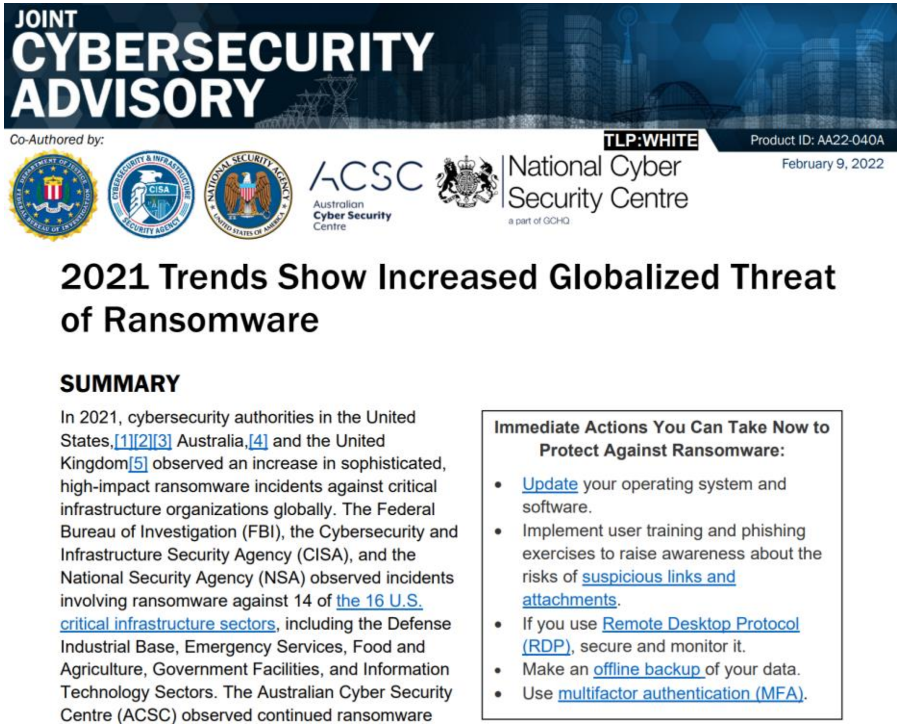
- True story: CandGrab RaaS admins RETIRED after making $2B
  - https://www.bankinfosecurity.com/ransomware-as-gandcrab-retires-sodinokibi-rises-a-12788



Ransomware Best Practices

- Eliminate or Secure RDP
- Offline Backups
- MFA
- Patch Management
- Social Engineering Training

Source



JOINT CYBERSECURITY ADVISORY

Co-Authored by:

ACSC Australian Cyber Security Centre

National Cyber Security Centre a part of GCHQ

TLP:WHITE

Product ID: AA22-040A

February 9, 2022

2021 Trends Show Increased Globalized Threat of Ransomware

SUMMARY

In 2021, cybersecurity authorities in the United States,[1][2][3] Australia,[4] and the United Kingdom[5] observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally. The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors, including the Defense Industrial Base, Emergency Services, Food and Agriculture, Government Facilities, and Information Technology Sectors. The Australian Cyber Security Centre (ACSC) observed continued ransomware

Immediate Actions You Can Take Now to Protect Against Ransomware:

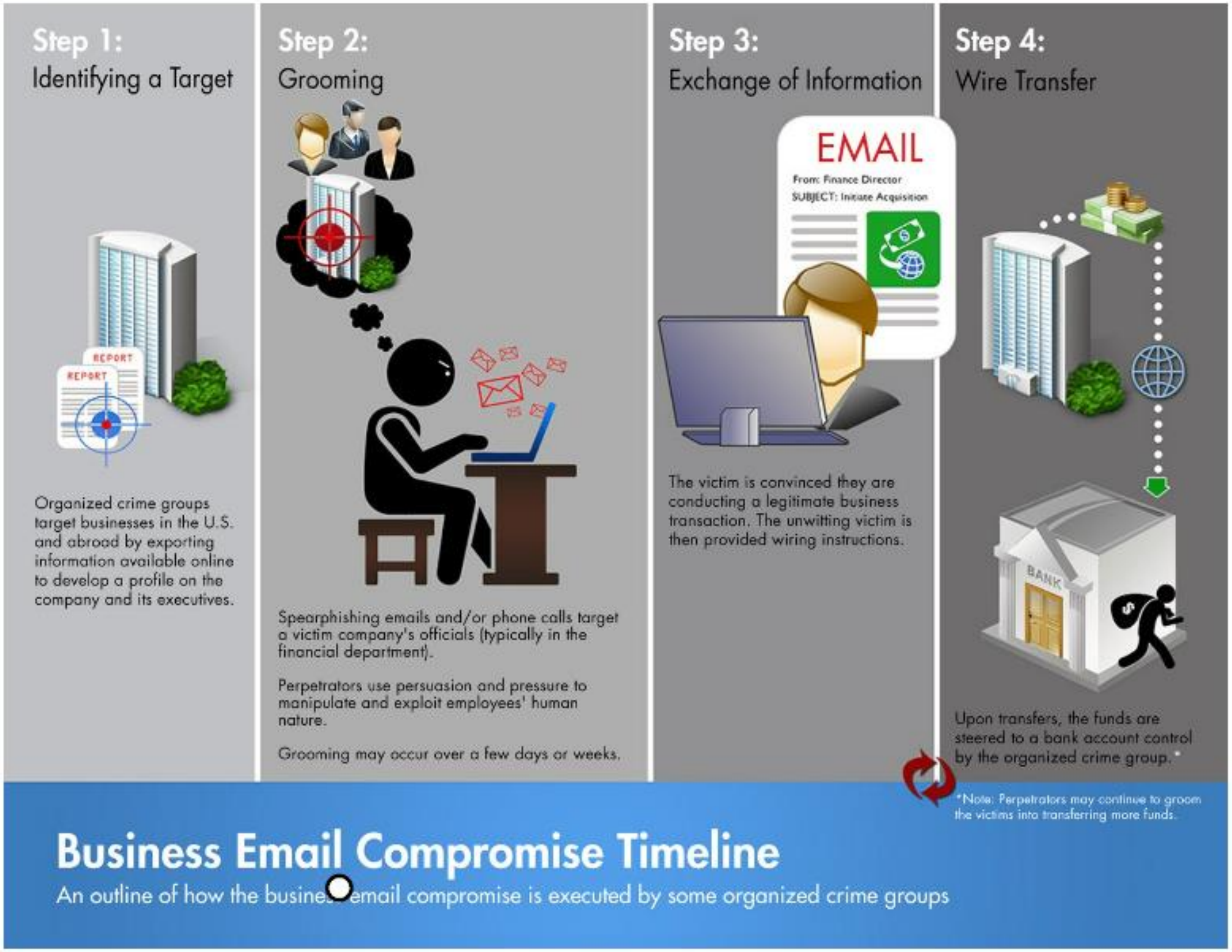
- Update your operating system and software.
- Implement user training and phishing exercises to raise awareness about the risks of suspicious links and attachments.
- If you use Remote Desktop Protocol (RDP), secure and monitor it.
- Make an offline backup of your data.
- Use multifactor authentication (MFA).

What’s in Your Email?

Email Compromise

- Business email compromise (BEC)
  - Hack into an executive or finance department email through phishing attempts
  - Spoof an email with a similar looking email
  - Create a domain and email format to look like the business
- BEC is used to gather data, convince someone to send money, or collect on a past due bill with instructions to send the money to the hacker account
- Vendor email compromise (VEC)
  - Same motivation as BEC but the fraud goes up stream and down stream.
  - Email attempts to customers and to your vendors vendor
- FinCEN says BEC nets an average of $50,000 and VEC nets an average of $125,000.

Business Email Compromise (BEC)



Step 1:
Identifying a Target

Organized crime groups target businesses in the U.S. and abroad by exporting information available online to develop a profile on the company and its executives.

Step 2:
Grooming

Spearphishing emails and/or phone calls target a victim company's officials (typically in the financial department).

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

Grooming may occur over a few days or weeks.

Step 3:
Exchange of Information

The victim is convinced they are conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4:
Wire Transfer

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

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

Business Email Compromise Timeline

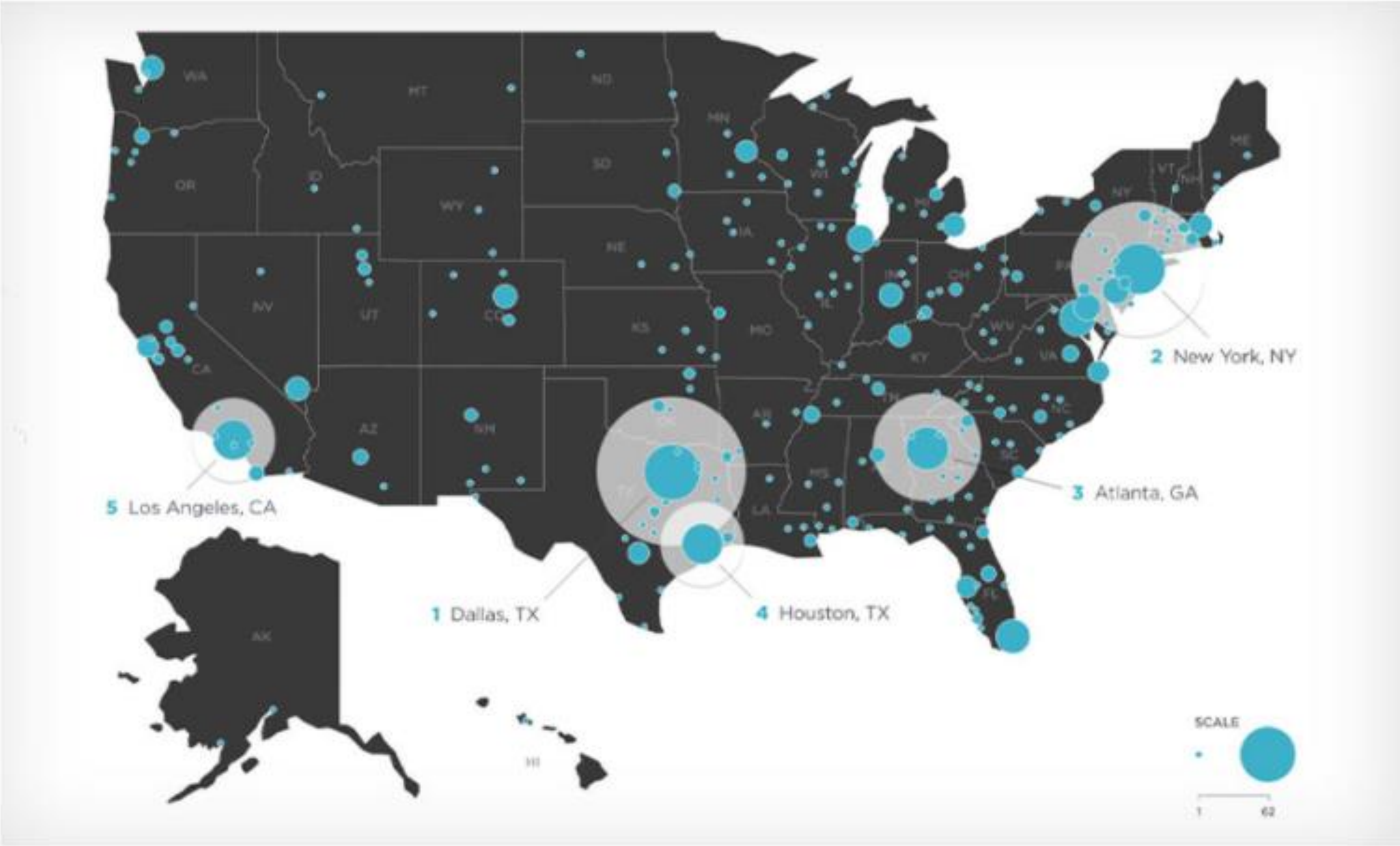
An outline of how the business email compromise is executed by some organized crime groups

BEC Red Flags

- Unusual and/or unexplained urgency
- Last minute changes in wire instructions or recipient account information
- Last minute changes in established communication platforms or email account addresses
- Communications only in email and **refusal to communicate via telephone** or online voice or video platforms
- Requests for advanced payment of services when not previously required
- Requests from employees to change direct deposit information

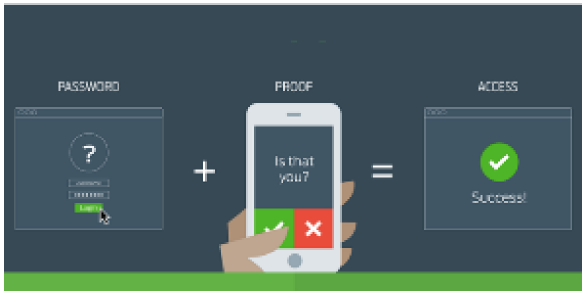
BEC Gangs Are US Based

- US Now Second to Nigeria for Business Email Compromise Fraudsters



This map shows locations of BEC criminal gangs in the U.S. (Source: Agari)

BEC Best Practices



- Know how to identify phished/spoofed emails
- Be careful about what is posted on social media
- Know your customer, ask questions.
  - They might not know they were tricked.
- Follow call-back procedures, **NEVER** transact based on an email.
  - Control changes to email, rules, and phone address
- Educate customers on:
  - Monitor for “urgent” requests
  - Verify changes to vendor (or employee) account information
  - Notify bank when suspicious activity occurs
- **ALWAYS ENABLE MULTIFACTOR AUTHENTICATION!**
  - **O365 include conditional access**

Account Takeover

Account takeover (ATO) occurs in several different ways:

- When criminals use stolen credentials to access a user's online accounts without permission.
- Cyber thieves create online accounts that users have not created:
  - Credit Cards
  - Credit Bureaus (Equifax, Experian, Transunion) and (National Consumer Telecommunications and Utilities Exchange, or nctue.com)
  - Social Security
  - IRS
  - Cell Phone/Utilities
  - Social Media

- **ALWAYS ENABLE MULTIFACTOR AUTHENTICATION!**

Corporate Account Takeover

- Cyber criminals gain control of a business' bank account by stealing the business' valid online banking credentials.
  - Deploy multifactor authentication for business account access
  - Should require payment initiation under dual control
  - Should have out-of-band confirmation of payment initiation
  - Should establish and monitor exposure limits

Your Risk

- More than 50% of all small businesses suffered a breach within the last year.
- Incidents cost businesses of all sizes $200,000 on average
- 66% of senior decision-makers at small businesses still believe they're unlikely to be targeted by online criminals.

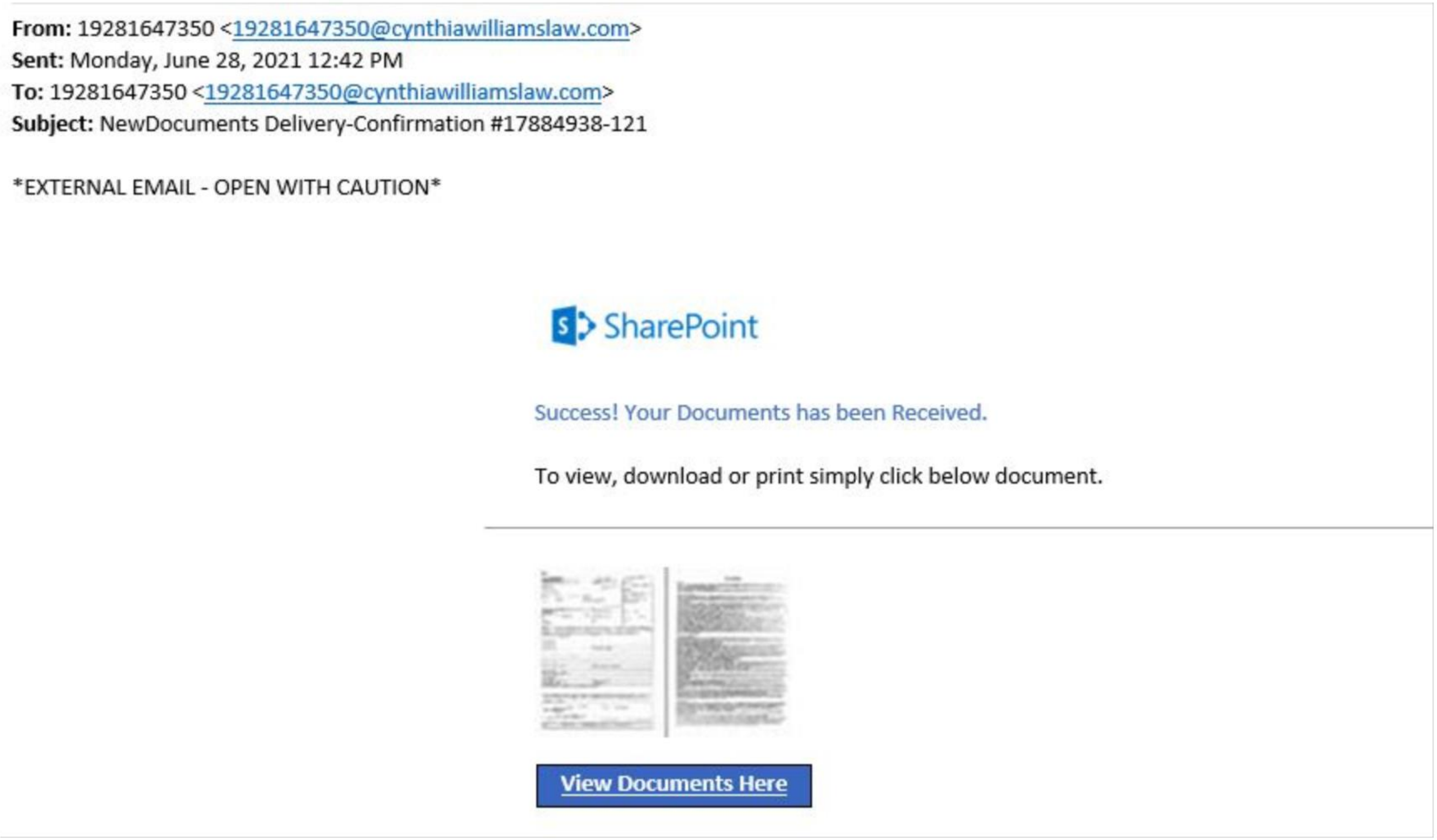
Source: CNBC

Social Engineering

How to Recognize Fake Emails

- An email should not solicit an emotional response!
- If you are not expecting the email be cautious.
- Sender address isn't correct
  - kschroll@nlnb.com vs
  - kschroll@nlb.com
  - Hover over links to see what URL the link takes you.
- Obvious grammar or spelling errors
- Strange structures
  - Generic greeting
  - Urgent language
  - Generic closing
- Your customers experience compromise and blame you. This can become reputational risk for the institution.

Phishing Example: SharePoint



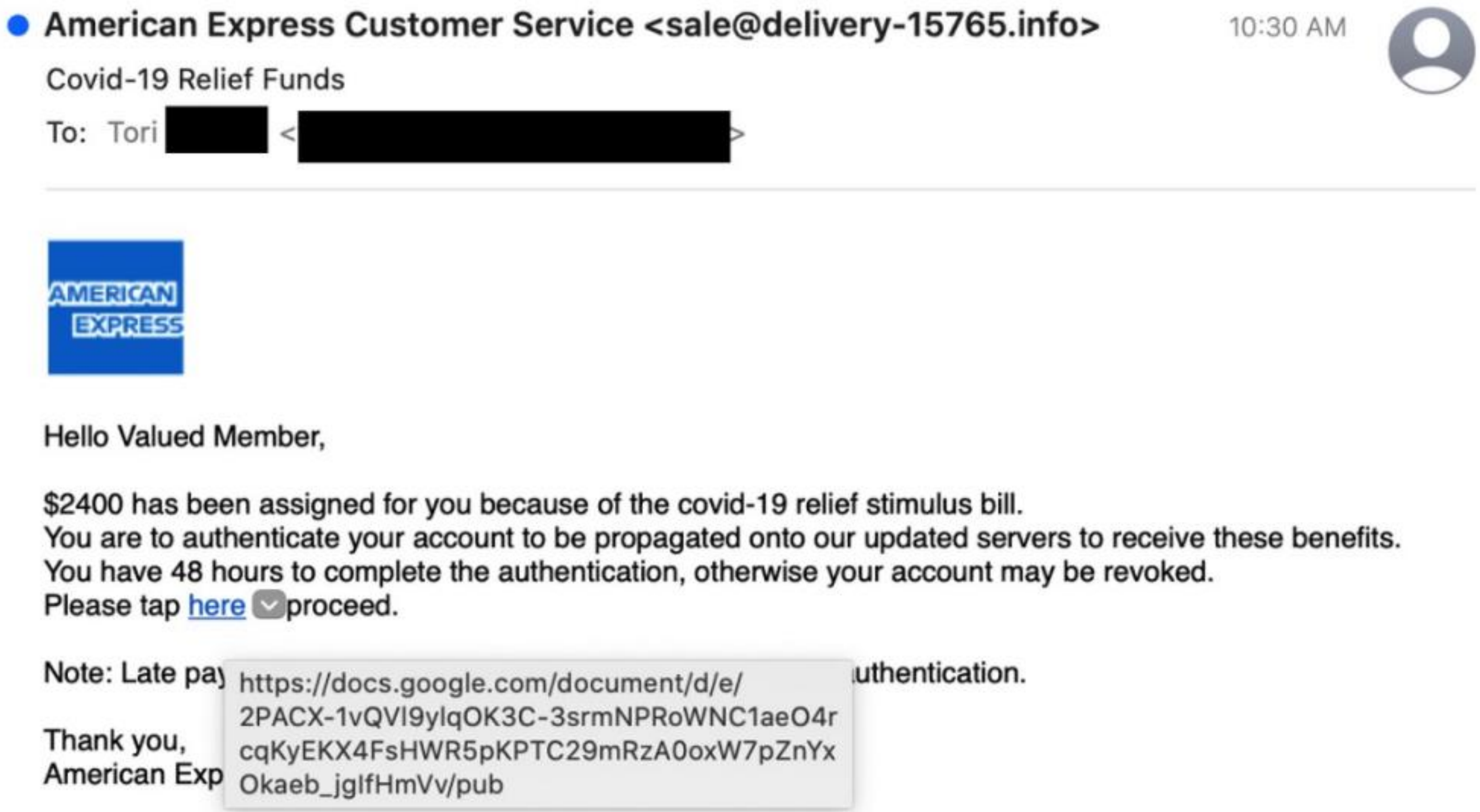
From: 19281647350 <19281647350@cynthiawilliamslaw.com>
Sent: Monday, June 28, 2021 12:42 PM
To: 19281647350 <19281647350@cynthiawilliamslaw.com>
Subject: NewDocuments Delivery-Confirmation #17884938-121

EXTERNAL EMAIL - OPEN WITH CAUTION

Success! Your Documents has been Received.

To view, download or print simply click below document.

Phishing Example: Stimulus



American Express Customer Service <sale@delivery-15765.info> 10:30 AM

Covid-19 Relief Funds

To: Tori [redacted] <[redacted]>

Hello Valued Member,

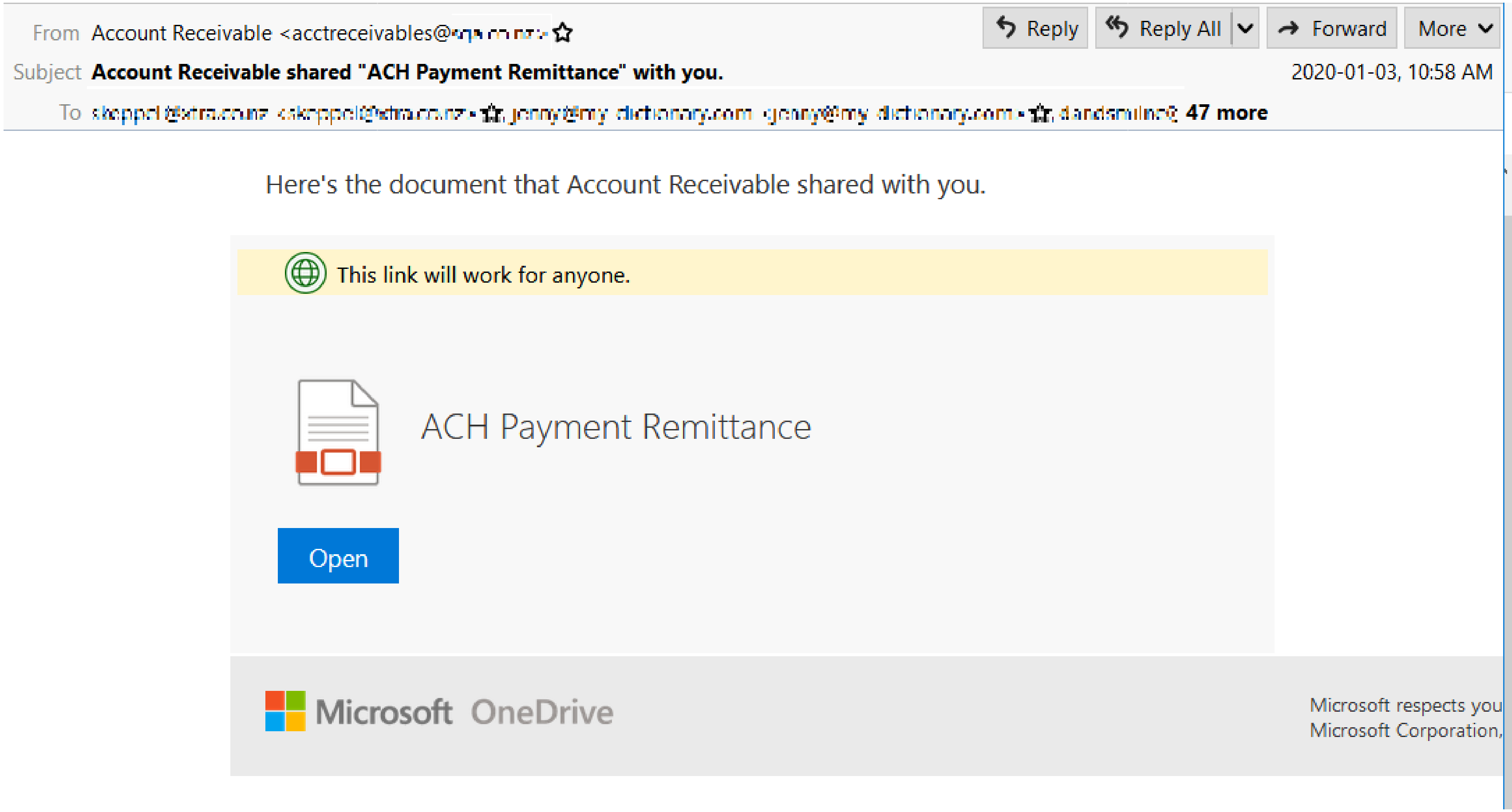
$2400 has been assigned for you because of the covid-19 relief stimulus bill.
You are to authenticate your account to be propagated onto our updated servers to receive these benefits.
You have 48 hours to complete the authentication, otherwise your account may be revoked.
Please tap here proceed.

Note: Late pay uthentication.

Thank you,
American Exp

https://docs.google.com/document/d/e/2PACX-1vQVl9ylqOK3C-3srmNPRoWNC1aeO4rcqKyEKX4FsHWR5pKPTC29mRzA0oxW7pZnYxOkaeb_jglfHmVv/pub

Difficult to identify?



From Account Receivable <acctreceivables@[redacted]>

Subject **Account Receivable shared "ACH Payment Remittance" with you.**

2020-01-03, 10:58 AM

To [redacted] **47 more**

Here's the document that Account Receivable shared with you.

This link will work for anyone.

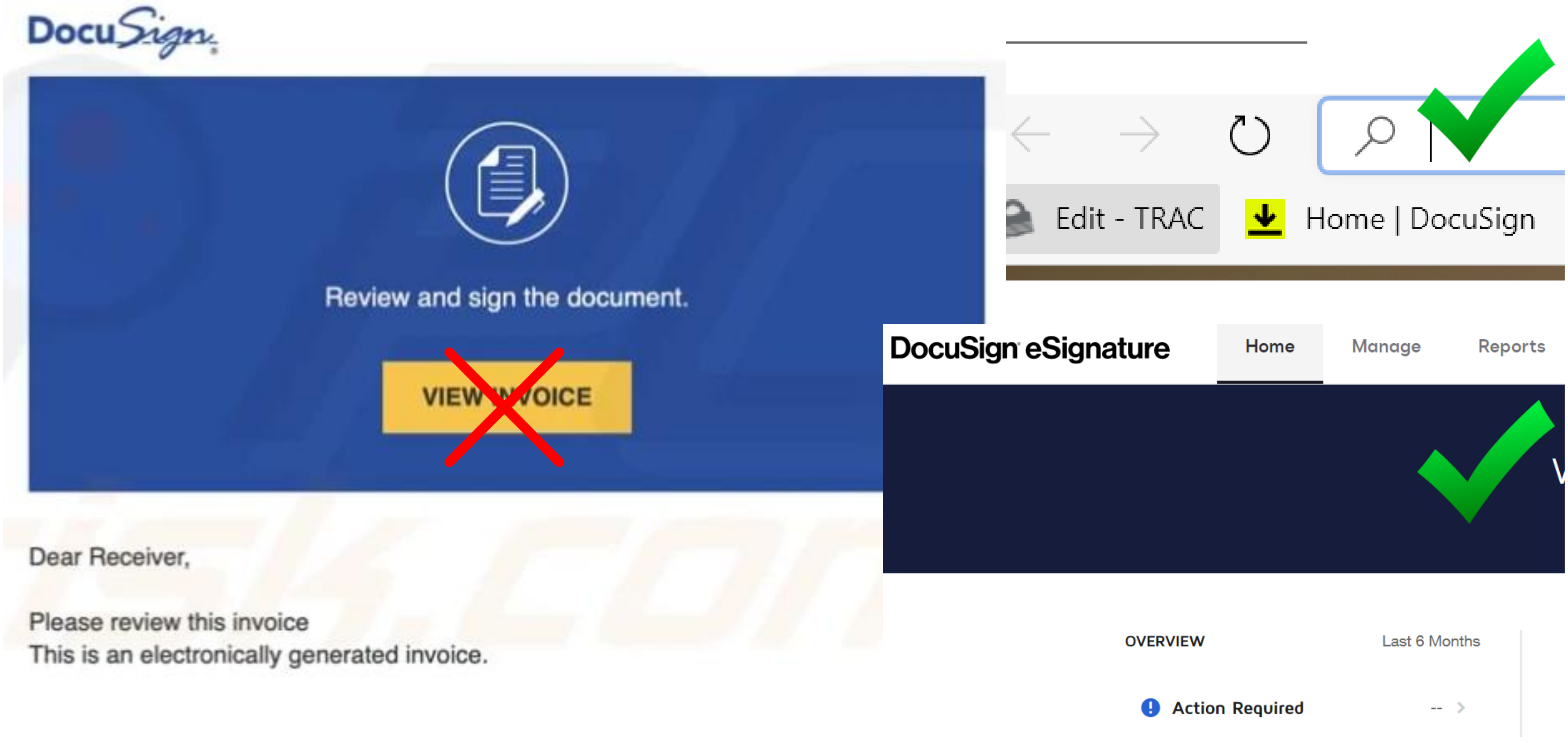
ACH Payment Remittance

Open

Microsoft OneDrive

Microsoft respects you
Microsoft Corporation,

Difficult to identify?

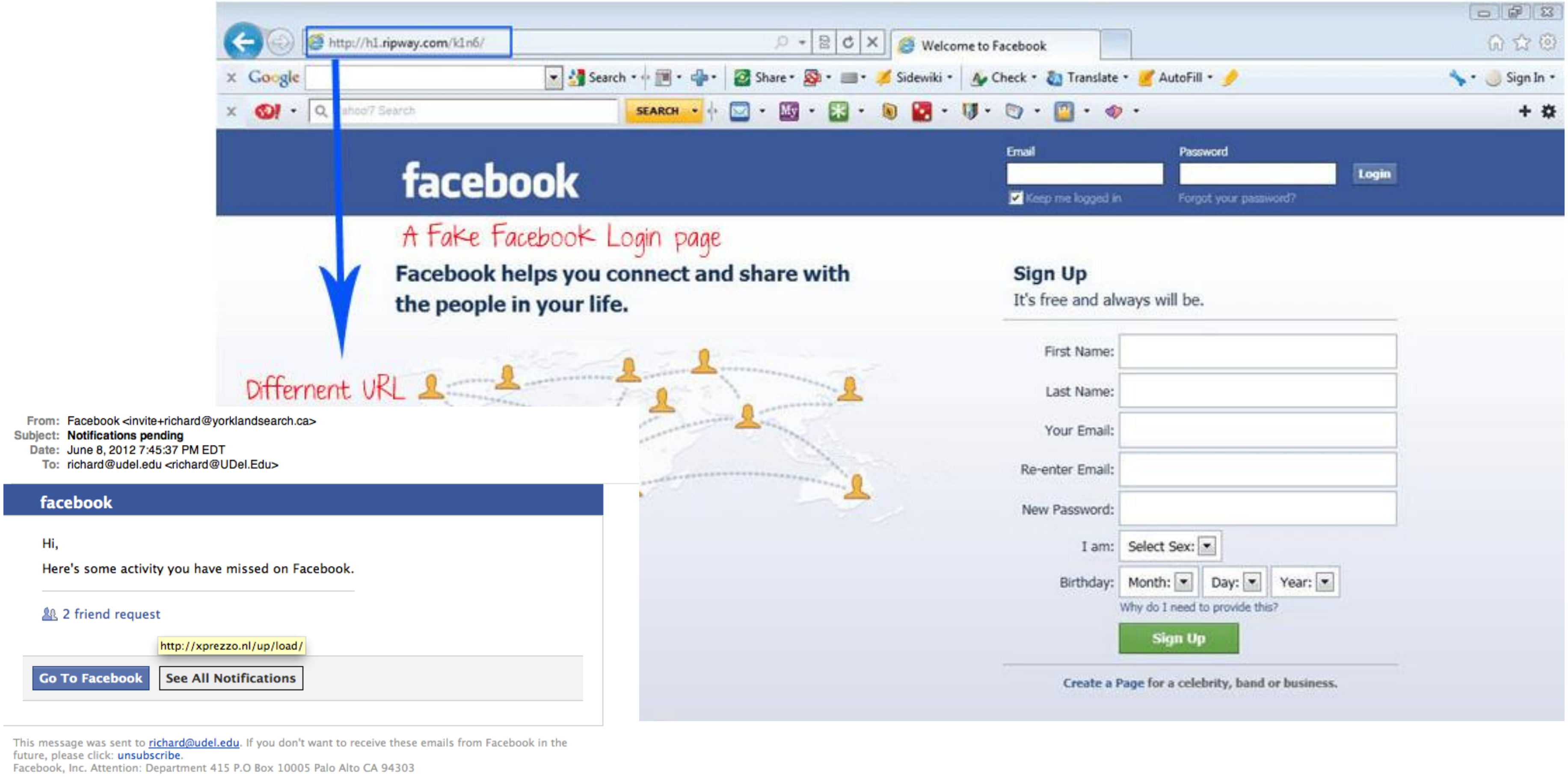


Review and sign the document.

Dear Receiver,

Please review this invoice
This is an electronically generated invoice.

Stealing Credentials



A Fake Facebook Login page

Facebook helps you connect and share with the people in your life.

Sign Up

It's free and always will be.

First Name:

Last Name:

Your Email:

Re-enter Email:

New Password:

I am: Select Sex:

Birthday: Month: Day: Year:

Why do I need to provide this?

Create a Page for a celebrity, band or business.

Different URL

From: Facebook <invite+richard@yorklandsearch.ca>
Subject: **Notifications pending**
Date: June 8, 2012 7:45:37 PM EDT
To: richard@udel.edu <richard@UDel.Edu>

Hi,

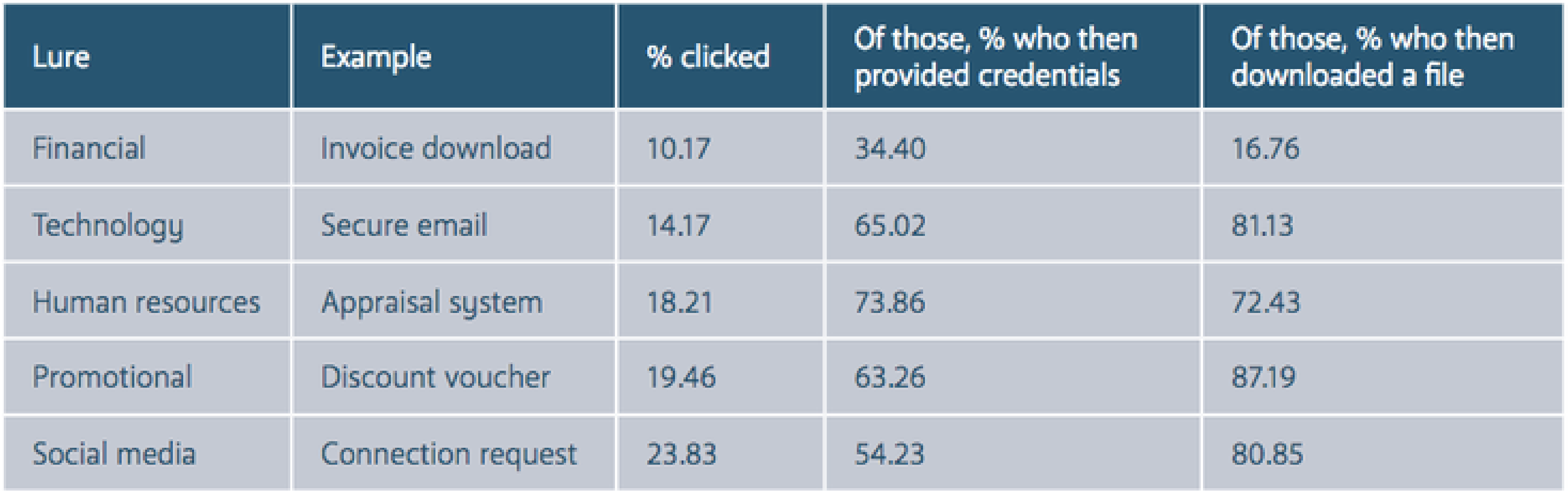
Here's some activity you have missed on Facebook.

2 friend request

http://xprezzo.nl/up/load/

This message was sent to richard@udel.edu. If you don't want to receive these emails from Facebook in the future, please click: unsubscribe.
Facebook, Inc. Attention: Department 415 P.O Box 10005 Palo Alto CA 94303

Popular Phishing Campaigns



Lure	Example	% clicked	Of those, % who then provided credentials	Of those, % who then downloaded a file
Financial	Invoice download	10.17	34.40	16.76
Technology	Secure email	14.17	65.02	81.13
Human resources	Appraisal system	18.21	73.86	72.43
Promotional	Discount voucher	19.46	63.26	87.19
Social media	Connection request	23.83	54.23	80.85

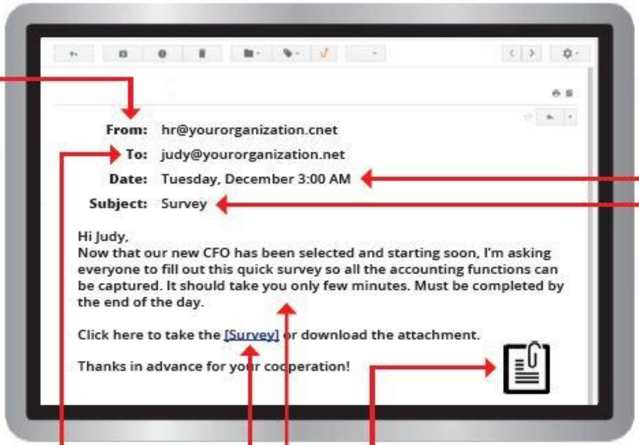
The effectiveness of a phishing campaign.

Source: MWR InfoSecurity

The Email Link

- https://sbscyber.com/
- https://www.apple.com/iphone/
- How do you know if these are legitimate links?
- VirusTotal, Google Safe Browsing, Norton Safe Web, Unmaskparasites.com
- Look to the right of “http(s)://” until you encounter the first forward slash (/)
- The domain directly to the left of that first slash is the true destination
- https://www.apple.com.example.com/findmyphone/
- The link above, example.com is the true destination, not apple.com

Social Engineering Red Flags



From: hr@yourorganization.cnet

To: judy@yourorganization.net

Date: Tuesday, December 3:00 AM

Subject: Survey

Hi Judy,
Now that our new CFO has been selected and starting soon, I'm asking everyone to fill out this quick survey so all the accounting functions can be captured. It should take you only few minutes. Must be completed by the end of the day.

Click here to take the [Survey] or download the attachment.

Thanks in advance for your cooperation!

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known website. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

© 2016–19 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

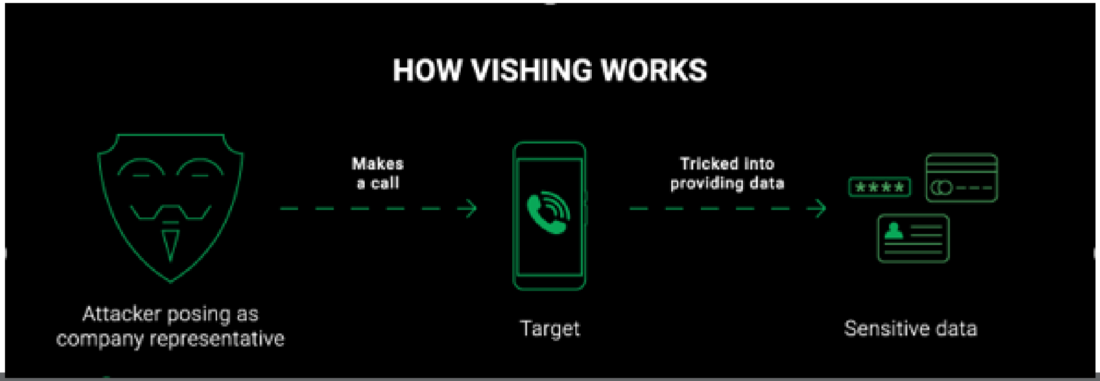
KnowBe4
Human error. Conquered.

What to Do with These Emails

- DO NOT CLICK ON ANY UNKNOWN LINKS!
- If you are not sure about the email, caution on the side of not clicking anything or opening attachments.
- Contact the ISO or a member of the IT Department to let them know about the email and they will let you know what to do with it.
- Training is VITAL!

Vishing

- Voice Phishing (i.e. robocalls)
- Often spoof Caller-ID
- Pose as a legitimate business to steal sensitive information over the phone or visit a website
- Famous examples:
  - Fake IRS “you’re going to jail” calls
  - Fake Microsoft Support “you’ve got a virus” calls
  - Fake Bank “your account has been compromised” calls

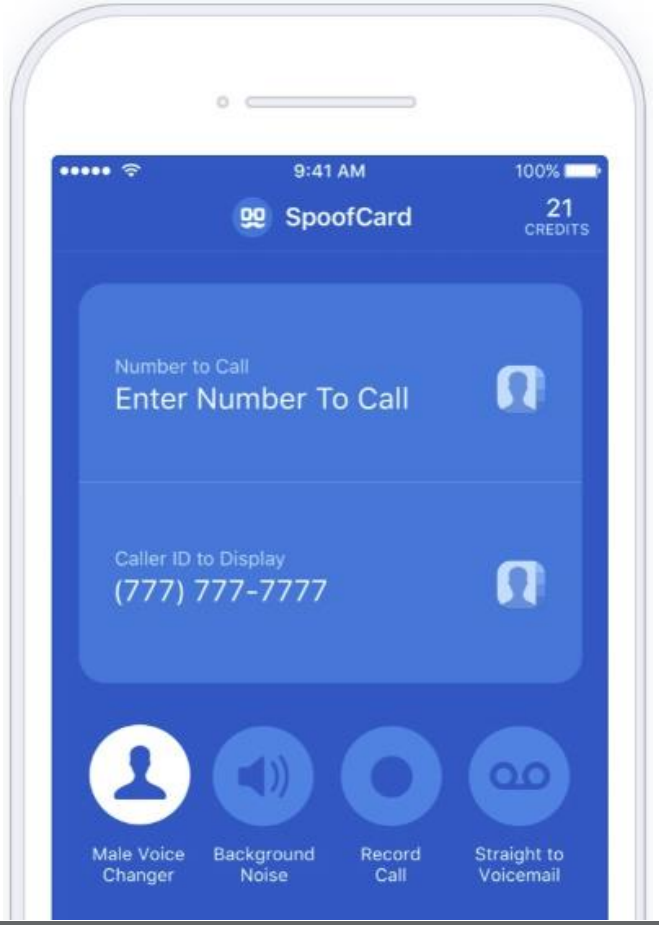


HOW VISHING WORKS

Attacker posing as company representative
Makes a call
Target
Tricked into providing data
Sensitive data

How Do You Identify someone?

- Can you use the caller ID on a phone call?
- If a caller knows the last four of a SS #, do you give them information?
- If a caller says they are with law enforcement or the government, do you give them information?



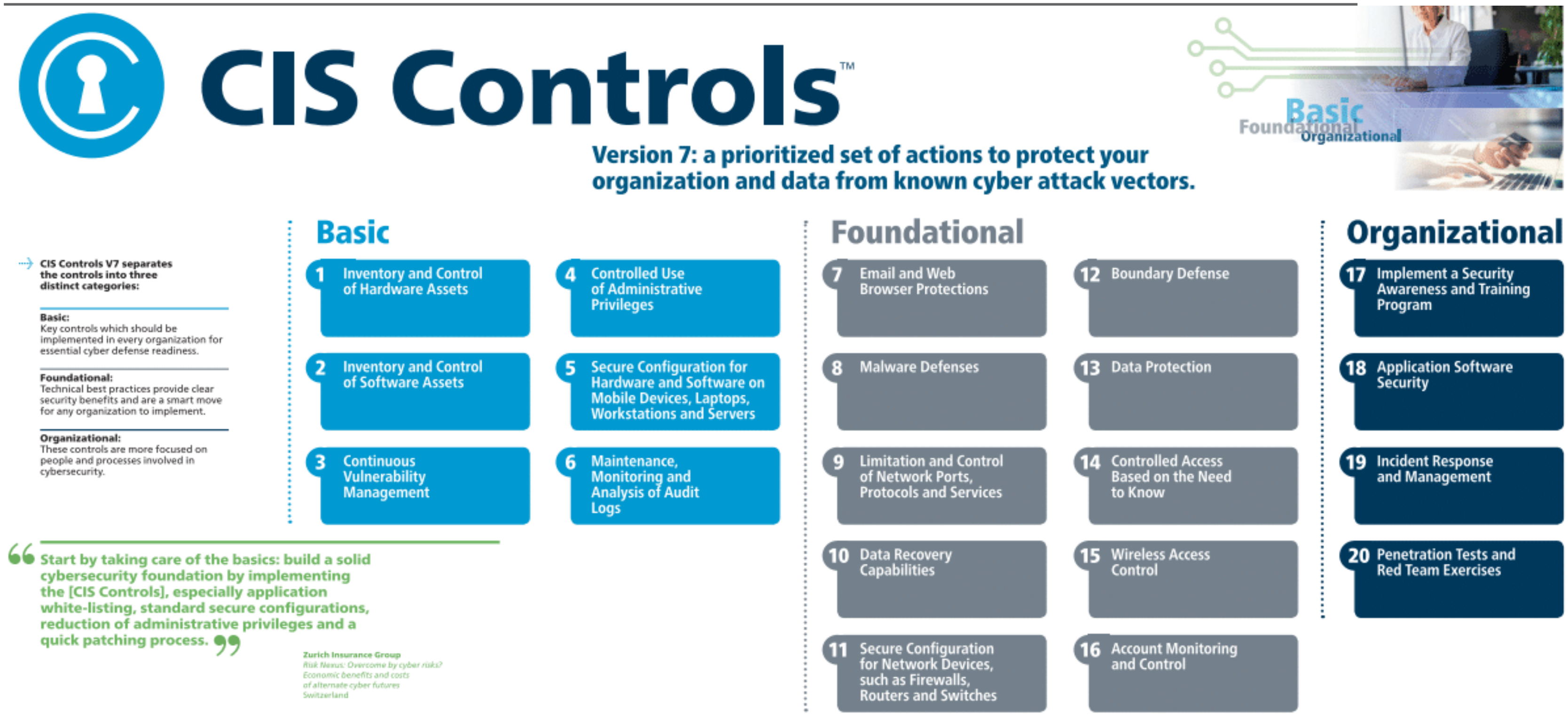
Number to Call
Enter Number To Call

Caller ID to Display
(777) 777-7777

Social Media and Work

- Secure Your Accounts – MFA, Restrict Visibility, Alerts
- Does your work allow you to identify yourself as an employee of the company on social media?
- Are there work approved online behaviors identified by your work?
- Are there consequences if you post inappropriate content on social media?
- When your reputation is at risk,
  your company's reputation is at risk!
- Social Media Policy

CIS Top 18 Cyber Controls


Basic
Foundational
Organizational

CIS Controls™

Version 7: a prioritized set of actions to protect your organization and data from known cyber attack vectors.

CIS Controls V7 separates the controls into three distinct categories:

Basic:
Key controls which should be implemented in every organization for essential cyber defense readiness.

Foundational:
Technical best practices provide clear security benefits and are a smart move for any organization to implement.

Organizational:
These controls are more focused on people and processes involved in cybersecurity.

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

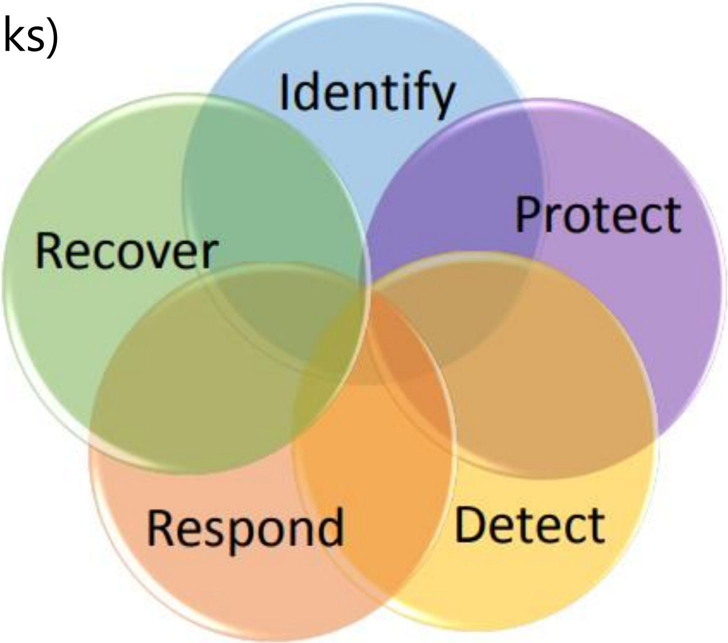
20 Penetration Tests and Red Team Exercises

> “Start by taking care of the basics: build a solid cybersecurity foundation by implementing the [CIS Controls], especially application white-listing, standard secure configurations, reduction of administrative privileges and a quick patching process.”

Zurich Insurance Group
Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures
Switzerland

Prevention

- NIST 7621 – Small Business Information Security Fundamentals
  - Identify
    - Know Employees (background checks)
    - Individual User Accounts
    - Identify and Control Access
    - Policies and Procedures
  - Protect
    - Restrict Access/Permissions
      - Strong Passwords and MFA
    - Surge Protectors/UPS
    - Patch OS and Applications
    - Firewalls (software and hardware)
      - Egress Filtering and Geo-blocking



© SBS CyberSecurity, LLC

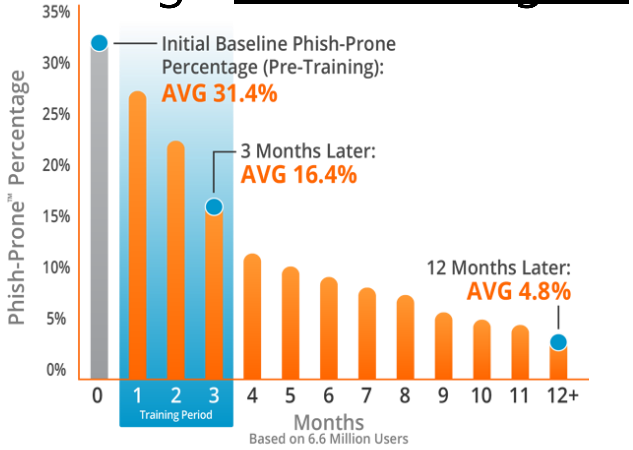
Prevention

- NIST 7621 – Small Business Information Security Fundamentals
  - Protect (continued)
    - Secure Wireless -
      - Admin password, WPA-2 w/AES, Guest Network, SSID, Update Firmware
    - Web and Email Filters
      - Content Filter, Spam Filter, DMARC, SPF, DKIM, Sandboxing
    - Encrypt Data and Email
      - Bitlocker, Secure Email
    - Dispose of Old Computers/MFP's/Equipment/Media Safely
    - Training – Cybersecurity Culture
      - Immediately at hire and annually (min)
      - Knowbe4
      - www.sba.gov/media/training/SBA_Cybersec/new/story_html5.html

Training

Train your employees

- Phishing #<u>1 and #2 largest </u>business risk



Source: 2021 KnowBe4 Phishing by Industry Benchmarking Report

Note: The initial Phish-Prone percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation.

Subsequent time periods reflect Phish-Prone percentages for the subset of users who received training with the KnowBe4 console.

KnowBe4
Human error. Conquered.

Phishing attacks account for more than **80% of reported security incidents.**

CSO Online

Prevention

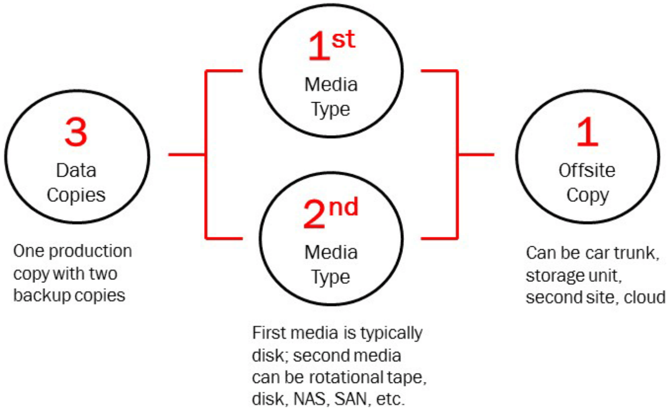
- NIST 7621 – Small Business Information Security Fundamentals
  - Detect
    - Install and update Anti-virus/Anti-Malware w/scripting control
      - CrowdStrike, Sentinel One
    - Maintain and Monitor Logs
  - Respond
    - Develop Plan (BCP, IRP, Pandemic)
  - Recover
    - Data Backups and TEST!
    - Cyber Insurance
    - Continually Advance/Improve Processes/Procedures/Technologies

- Additional Best Practices
  - Vendor Management and Restrict Access
  - O365 Security - (sbscyber.com)
  - Utilize results to enhance security

Backups are Critical

Make incremental backups of important business data/information

- Ensure they are complete and work. **Test.**
- Keep copies **offline** (Ransomware Proof)
- Make copies often. How much can you loose?
- Replication doesn't count.



3 Data Copies

One production copy with two backup copies

1st Media Type

2nd Media Type

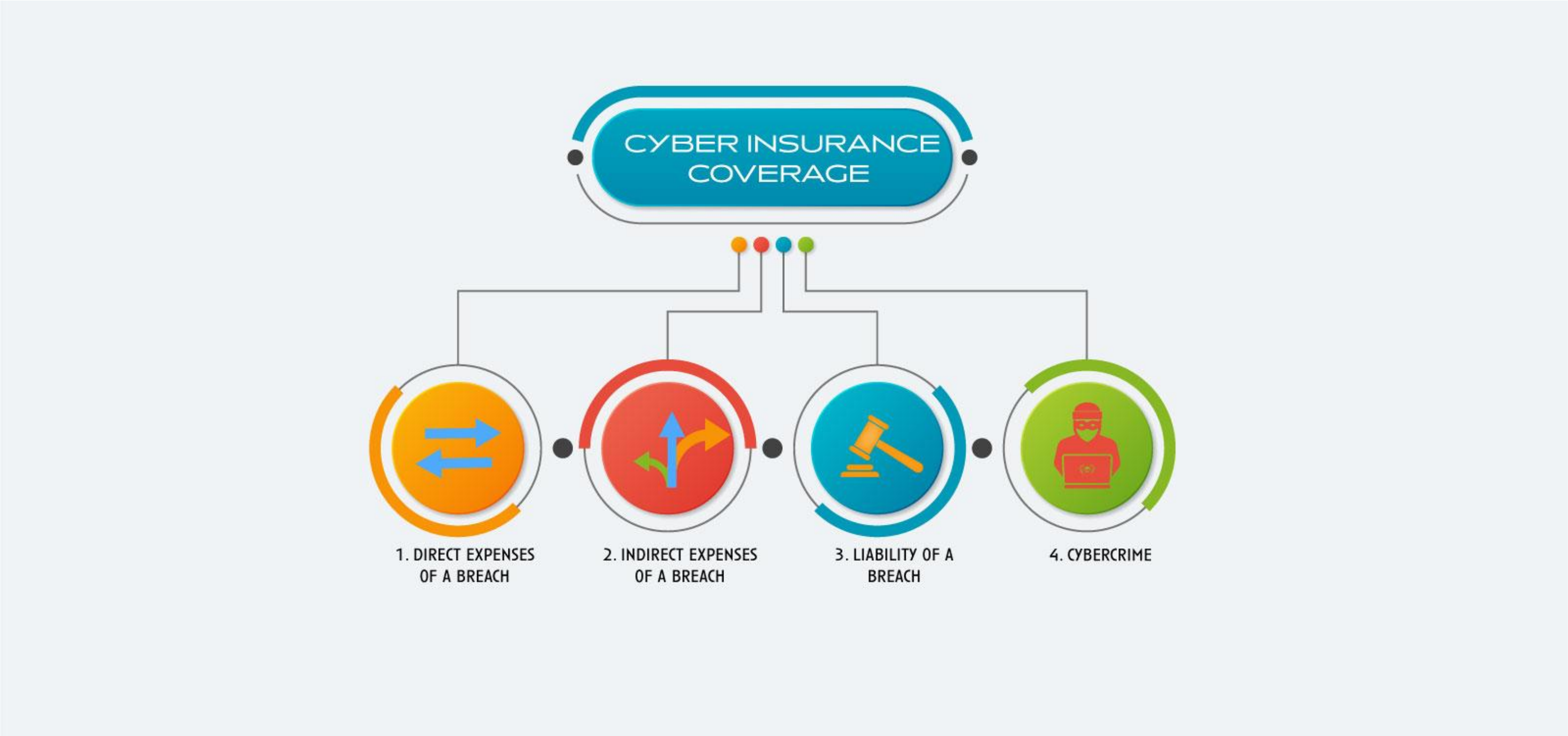
First media is typically disk; second media can be rotational tape, disk, NAS, SAN, etc.

1 Offsite Copy

Can be car trunk, storage unit, second site, cloud

Cyber Insurance

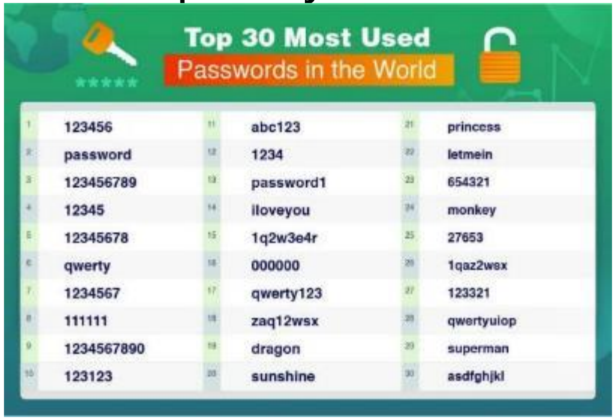
Consider cyber insurance – Getting $$$


CYBER INSURANCE COVERAGE
1. DIRECT EXPENSES OF A BREACH
2. INDIRECT EXPENSES OF A BREACH
3. LIABILITY OF A BREACH
4. CYBERCRIME

Password Guidelines

Use strong passwords

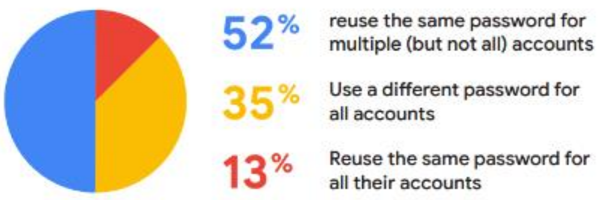
- Defaults – Change Them
- Reuse – Never Reuse
- Complexity – Make LONG



Top 30 Most Used
Passwords in the World

1	123456	11	abc123	21	princess
2	password	12	1234	22	letmein
3	123456789	13	password1	23	654321
4	12345	14	iloveyou	24	monkey
5	12345678	15	1q2w3e4r	25	27653
6	qwerty	16	000000	26	1qaz2wsx
7	1234567	17	qwerty123	27	123321
8	111111	18	zaq12wsx	28	qwertyuiop
9	1234567890	19	dragon	29	superman
10	123123	20	sunshine	30	asdfghjkl

Password reuse is still a common practice



52% reuse the same password for multiple (but not all) accounts

35% Use a different password for all accounts

13% Reuse the same password for all their accounts

onelogin

1Password

dashlane

LastPass •••|

RoboForm

How to Manage Passwords

- Avoid writing down (No sticky note and placing on monitor or under keyboard)
- Do not share with anyone, ever
- Avoid Excel

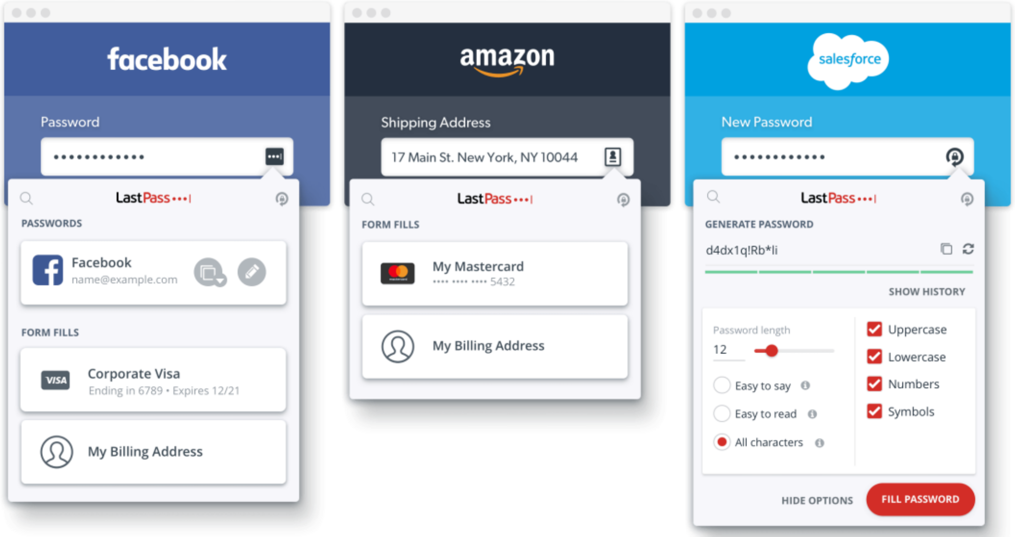
KEEPER Cybersecurity Starts Here™ ✓

RoboForm ✓

KeePass ✓

dashlane ✓

1Password ✓



facebook

Password

•••••••••••••

LastPass•••|

PASSWORDS

Facebook
name@example.com

FORM FILLS

Corporate Visa
Ending in 6789 • Expires 12/21

My Billing Address

amazon

Shipping Address

17 Main St. New York, NY 10044

LastPass•••|

FORM FILLS

My Mastercard
•••• •••• •••• 5432

My Billing Address

salesforce

New Password

•••••••••••••

LastPass•••|

GENERATE PASSWORD

d4dx1q!Rb*li

SHOW HISTORY

Password length

12

○ Easy to say

○ Easy to read

● All characters

☑ Uppercase

☑ Lowercase

☑ Numbers

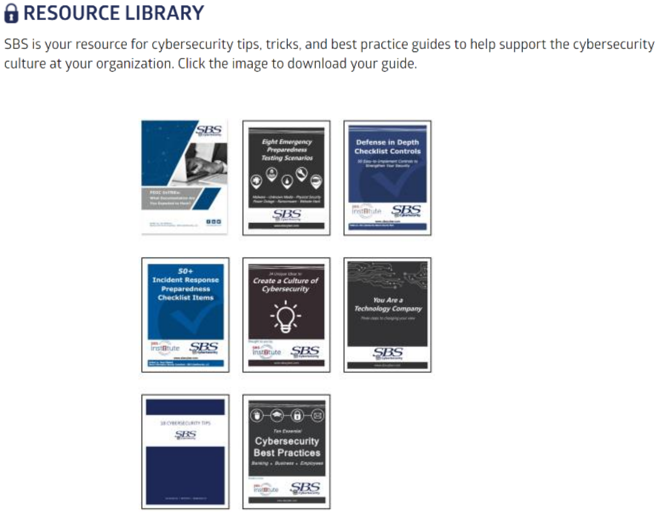
☑ Symbols

HIDE OPTIONS

FILL PASSWORD

Be Prepared – Incident Response

- Consider a tabletop test – roleplay ransomware
  - SBS Testing Example – various testing scenarios
  - Testing video - Successful Tabletop Testing Strategies
- Document a Plan
- Learn from other businesses incidents



RESOURCE LIBRARY

SBS is your resource for cybersecurity tips, tricks, and best practice guides to help support the cybersecurity culture at your organization. Click the image to download your guide.

SBS
Eight Emergency Preparedness Testing Scenarios
Malware - Unknown Media - Physical Security
Power Outage - Ransomware - Website Hack
Defense in Depth Checklist Controls
50+ Incident Response Preparedness Checklist Items
Create a Culture of Cybersecurity
You Are a Technology Company
10 CYBERSECURITY TIPS
Ten Essential Cybersecurity Best Practices
Banking • Business • Employees

Incident Response

- **Key items to report:**
  - Malicious Software
  - Unauthorized Access
  - Inappropriate Usage
  - Lost / Stolen Device
  - Service Provider breach (credit/debit card)
- **For every incident:**
  - Step 1: Report the incident to the Information Security Officer (ISO)

Your part in security is to:

REPORT ALL SUSPICIOUS ACTIVITY!

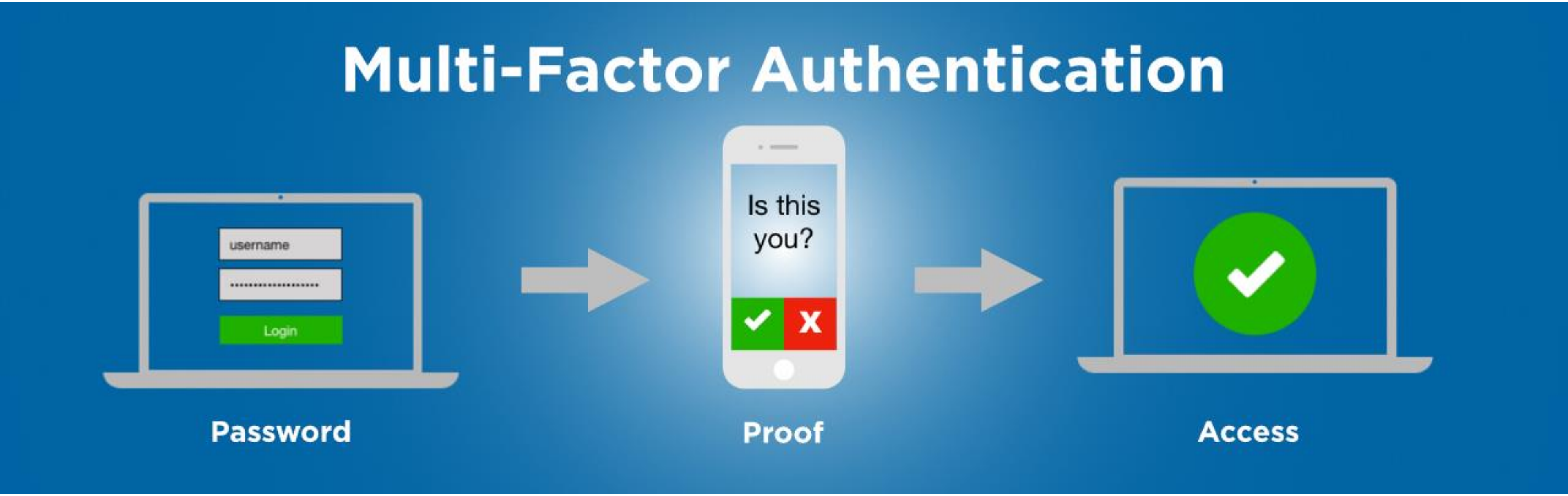
What is Multifactor Authentication?

What works as a factor of authentication?

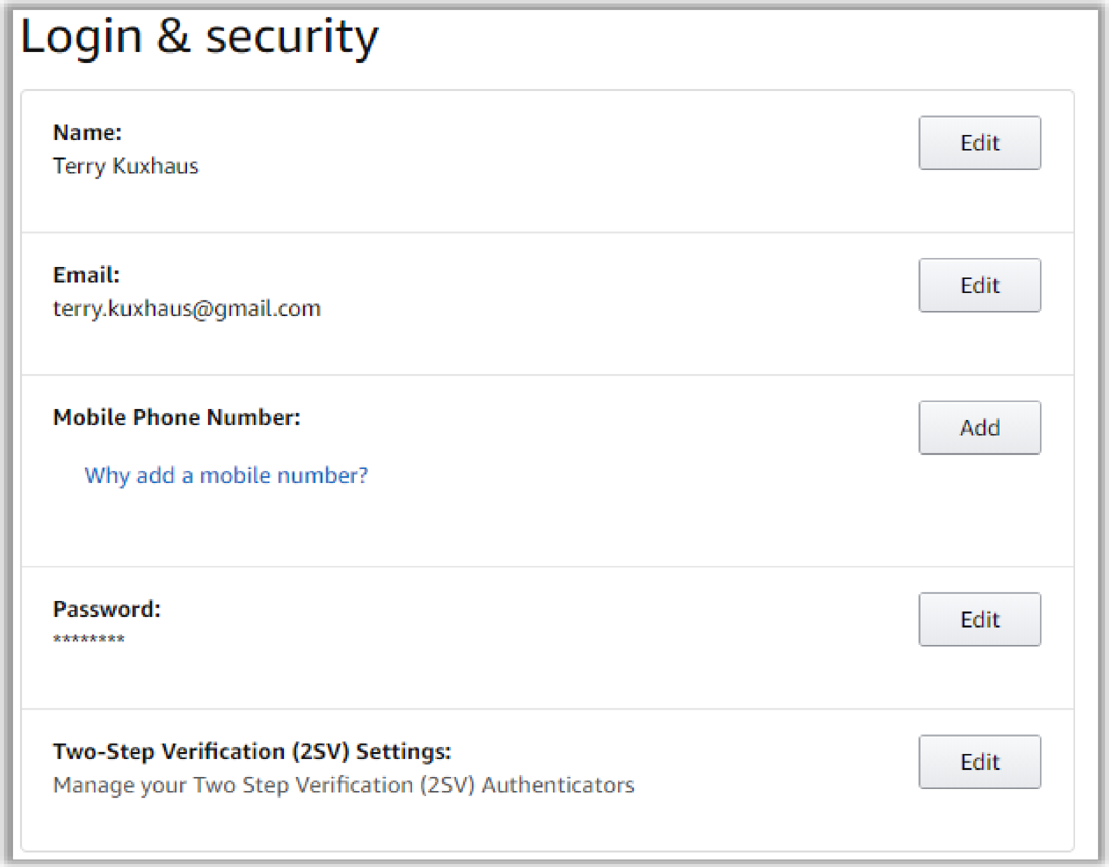
- Something you know – This is the most common factor and is easier to compromise. These are usernames, passwords, personal identification number (PIN), or security questions.
- Something you have – Hardware token or a One-time passcode. A less secure item is a hardware cookie on your device. The hardware cookie may easily be compromised.
- Something you are – Fingerprints, hand geometry, retinal or iris scans, handwriting, and voice analysis.

Multi-Factor Authentication

Multi-Factor is a great way to reduce risk of unauthorized access. But like most things Cybersecurity, it can be beaten.



Amazon Multifactor



Login & security

Name:
Terry Kuxhaus

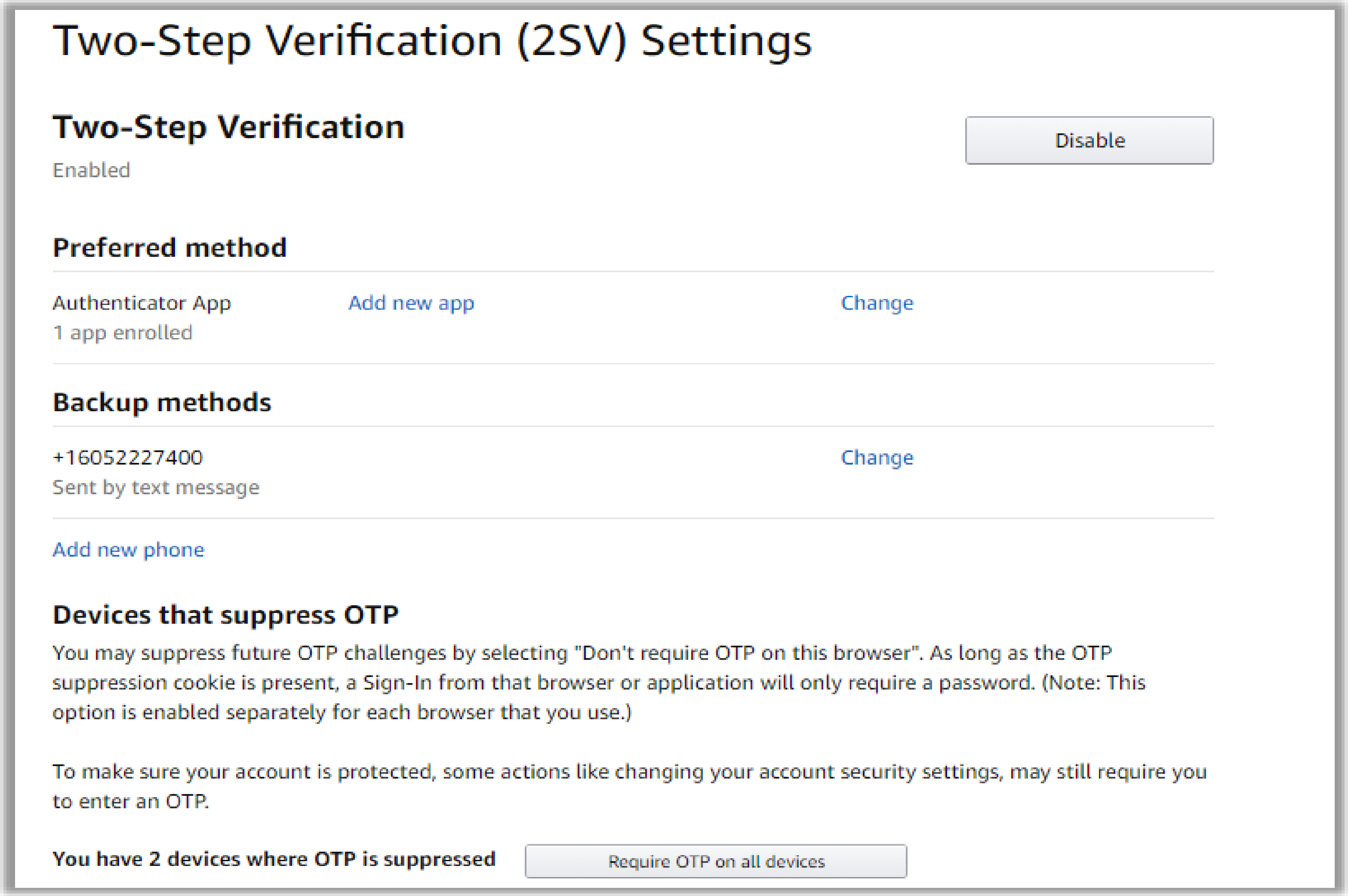
Email:
terry.kuxhaus@gmail.com

Mobile Phone Number:

Why add a mobile number?

Password:
****

Two-Step Verification (2SV) Settings:
Manage your Two Step Verification (2SV) Authenticators



Two-Step Verification (2SV) Settings

Two-Step Verification

Enabled

Preferred method

Authenticator App
1 app enrolled

Backup methods

+16052227400
Sent by text message

Devices that suppress OTP

You may suppress future OTP challenges by selecting "Don't require OTP on this browser". As long as the OTP suppression cookie is present, a Sign-In from that browser or application will only require a password. (Note: This option is enabled separately for each browser that you use.)

To make sure your account is protected, some actions like changing your account security settings, may still require you to enter an OTP.

You have 2 devices where OTP is suppressed

Mobile Device Threats

- Social engineering – phishing, smishing and vishing
- Wireless network security
- Out of date OS or applications
- Data leakage – personal cloud storage mixing with business information
- Bring your own device challenges
- Poor password hygiene or no password
- Physical device breaches
- Mobile advertising fraud
- Smishing

Smishing

- Prompt to click a link
- Request personal information or credentials
- Various scams, i.e. Stimulus Money
- Install Mobile Malware
- **Protection**
    - Never reply or click link
    - Look out for broken grammar, unnatural language
    - Only download apps from app store
    - Watch out for impersonation of Banks, CC, even Amazon
    - Urgent alerts, offers, etc.

How to Protect Yourself

- Controls to mitigate the risks to mobile devices can include:
  - Implementing a mobile device management system.
  - Ensuring mobile devices have anti-virus/anti-malware installed.
  - Ensuring mobile devices and applications are patched/updated.
  - User education on different social engineering tactics.
  - User education on safe browsing habits through the mobile device.
  - Encrypting the mobile device to protect against being lost or stolen.
  - Screen lock is required using a secure password or biometric to unlock the device.
  - Never share device or password with anyone.
  - Do not save confidential data on device if possible.
  - Do not use open WiFi.
  - Personal device - backup data to cloud and enable find my device.
- If lost or stolen?

Physical Security

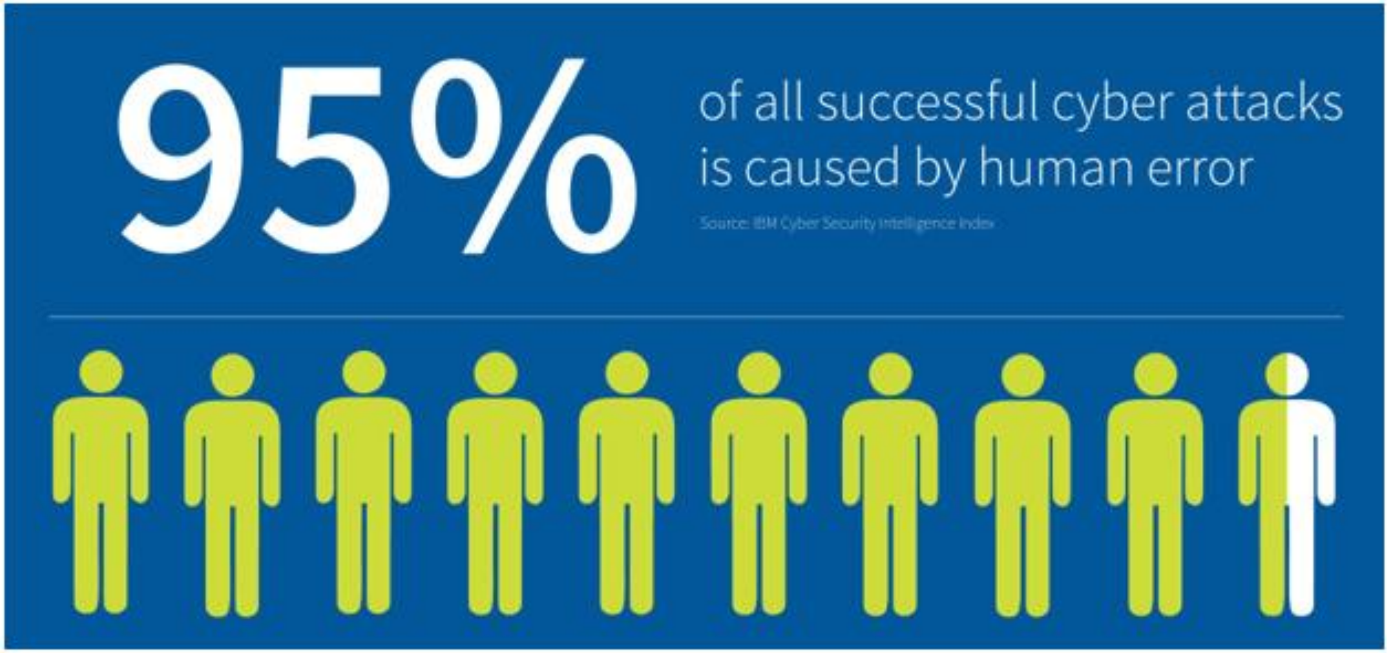
- Removeable media ports are blocked on your computer for a reason.
- Be on the lookout for shoulder surfing.
- Do not leave written passwords on your desk.
- Lock your computer screen when you walk away from your desk.
- Do not leave a phone that has access to Bank information out in plain sight.
- Secure confidential documentation, do not leave them visible on your desk.
- Shred confidential documentation

Remote Workforce Security

- Define Usage Guidelines – Acceptable Use Agreement
- VPN (virtual private network), Cloud Access, Desktop Sharing
    - No RDP without VPN
- Enforce Strong Passwords with MFA- Password Vault
- Protect Endpoints – Manage via the Cloud
    - Cylance, Sentinel One – Anomaly based with scripting control
    - Patching Process/Requirement
    - Web Filtering
    - Centralized logging
- No Personal PCs
    - Managed Devices - For Employees Only
    - O365 Conditional Access
- No Open Wi-Fi
- Encrypt Stored Data
- Restrict USB Storage
- Educate – Social Engineering, Malicious Activity

Human Firewall

You are the last line of defense in a cybersecurity attack!



of all successful cyber attacks is caused by human error

Source: IBM Cyber Security Intelligence Index

It is Up to YOU!