B.E.E.C.

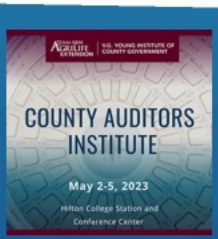
Beware Everyone or Everything is (possibly) Compromised

WHO & WHAT?

BEC

MITIGATION

WRAPPING IT UP



Texas A&M AgriLife Extension | V.G. Young Institute of County Government

COUNTY AUDITORS INSTITUTE

May 2-5, 2023

Hilton College Station and Conference Center

Robert Ruiz, ARM-P, AIC, CRM, CIC
May 3, 2023

DISCLAIMER

The information presented in this session is for educational purposes only. Possible claim scenarios discussed are hypothetical and are not official coverage determinations. Coverage as provided by TAC Risk Management Pool (TAC RMP) is subject to the terms and conditions of the specific coverage document.

Items presented are best practices only and are not a requirement of TAC RMP coverage *(at this time)*. TAC is not endorsing any software, services or technology companies, if referenced in this presentation.

This training does not satisfy or comply with HB3834 (86th Legislature) or any state statute requiring cybersecurity training.

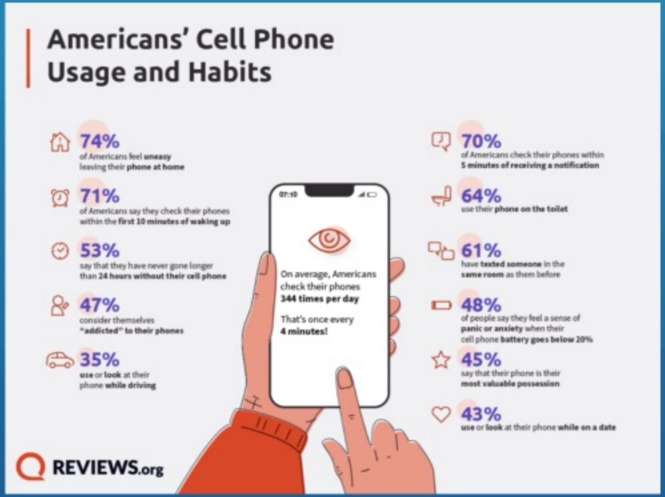
For Today...

- What is eCrime?
- Who is the perpetrator of an eCrime?
- How do they execute an eCrime?
- Who is the target of an eCrime?
- Steps to prevent and limit eCrime activities in your office

Why is eCrime so rampant?

Our world is becoming more connected and therefore smaller every day.

- Internet use continues to rise
- Internet has changed how we communicate
- Expansion of e-commerce
- Social media proliferation
- Mobile device use and ownership rapidly increasing as is our dependency on our phones!



Americans' Cell Phone Usage and Habits

74% of Americans feel **uneasy** leaving their **phone at home**

71% of Americans say they check their phones within the **first 10 minutes of waking up**

53% say that they have never gone longer than **24 hours without their cell phone**

47% consider themselves **"addicted" to their phones**

35% **use** or **look** at their phone **while driving**

On average, Americans check their phones **344 times per day**

That's once every **4 minutes!**

70% of Americans check their phones within **5 minutes of receiving a notification**

64% use their **phone on the toilet**

61% have **texted someone** in the **same room** as them before

48% of people say they feel a sense of **panic or anxiety** when their cell phone **battery goes below 20%**

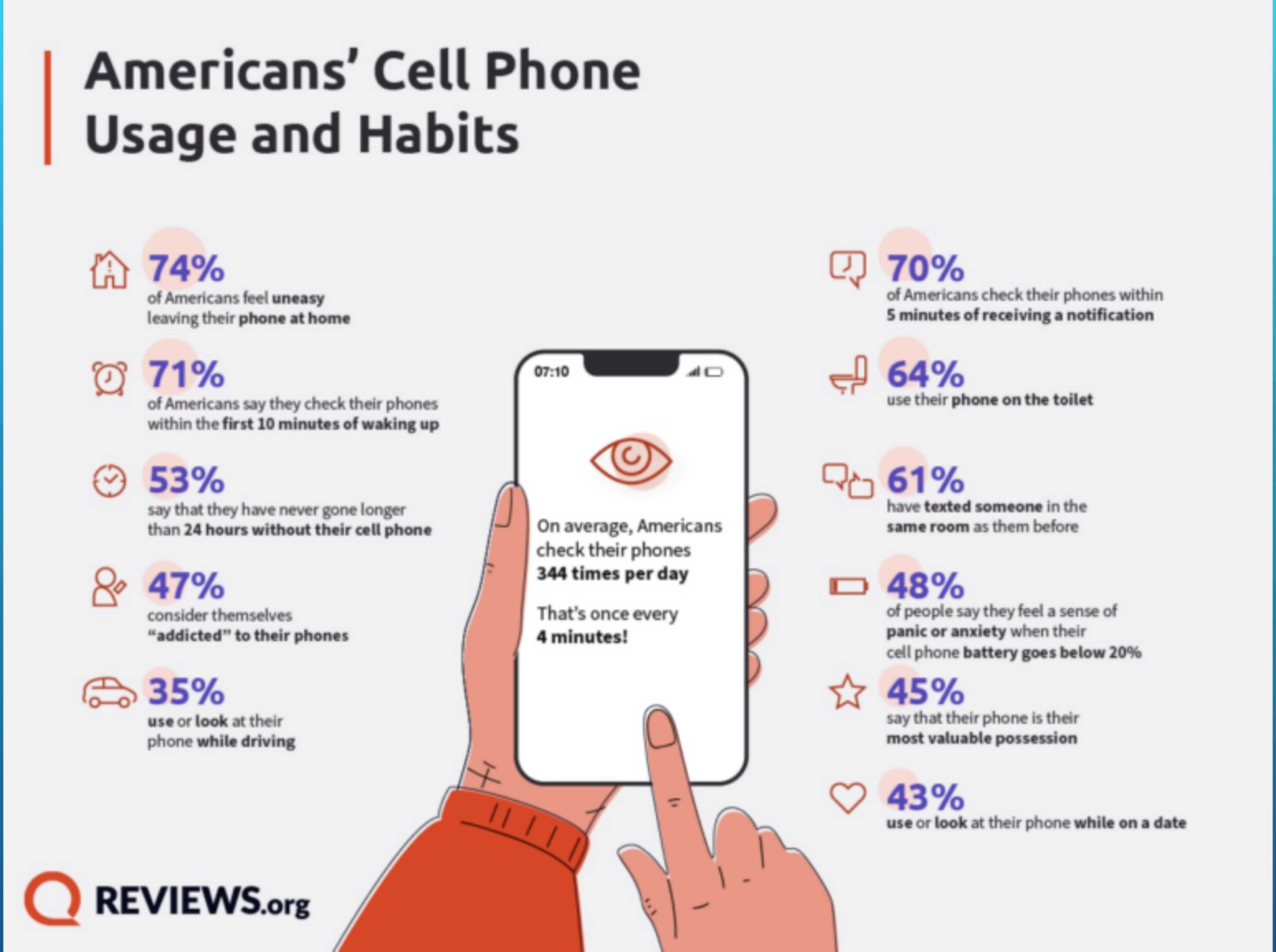
45% say that their phone is their **most valuable possession**

43% **use** or **look** at their phone **while on a date**

REVIEWS.org

What is eCrime?

Cyber Threat Actors



Americans' Cell Phone Usage and Habits

74%
of Americans feel **uneasy** leaving their **phone at home**

71%
of Americans say they check their phones within the **first 10 minutes of waking up**

53%
say that they have never gone longer than **24 hours without their cell phone**

47%
consider themselves **"addicted" to their phones**

35%
use or **look** at their phone **while driving**

07:10

On average, Americans check their phones **344 times per day**

That's once every **4 minutes!**

70%
of Americans check their phones within **5 minutes of receiving a notification**

64%
use their **phone on the toilet**

61%
have **texted someone** in the **same room** as them before

48%
of people say they feel a sense of **panic or anxiety** when their cell phone **battery goes below 20%**

45%
say that their phone is their **most valuable possession**

43%
use or **look** at their phone **while on a date**

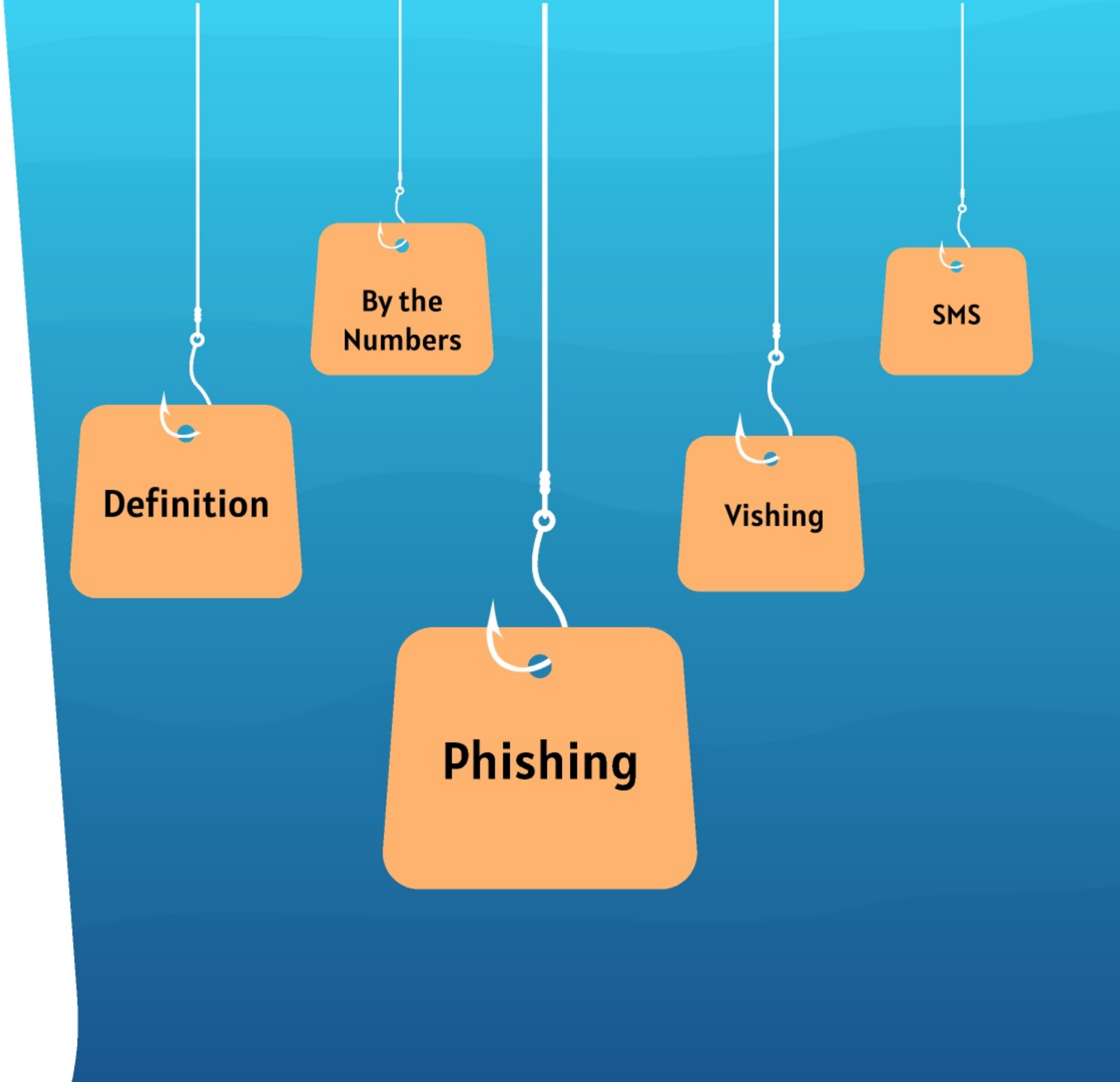
REVIEWS.org

eCrime = "Cyber Financial Fraud"

Of late and as seen in court cases, BEC is starting to be called ***'cyber-enabled financial fraud'*** (Poireault, InfoSecurity 12.27.2002).

Cyber crime is synonymous with eCrime

The FBI categorizes eCrime into **6 types** that threat actors will use against organizations, individuals, business and the general public.



Definition

By the Numbers

Phishing

Vishing

SMS

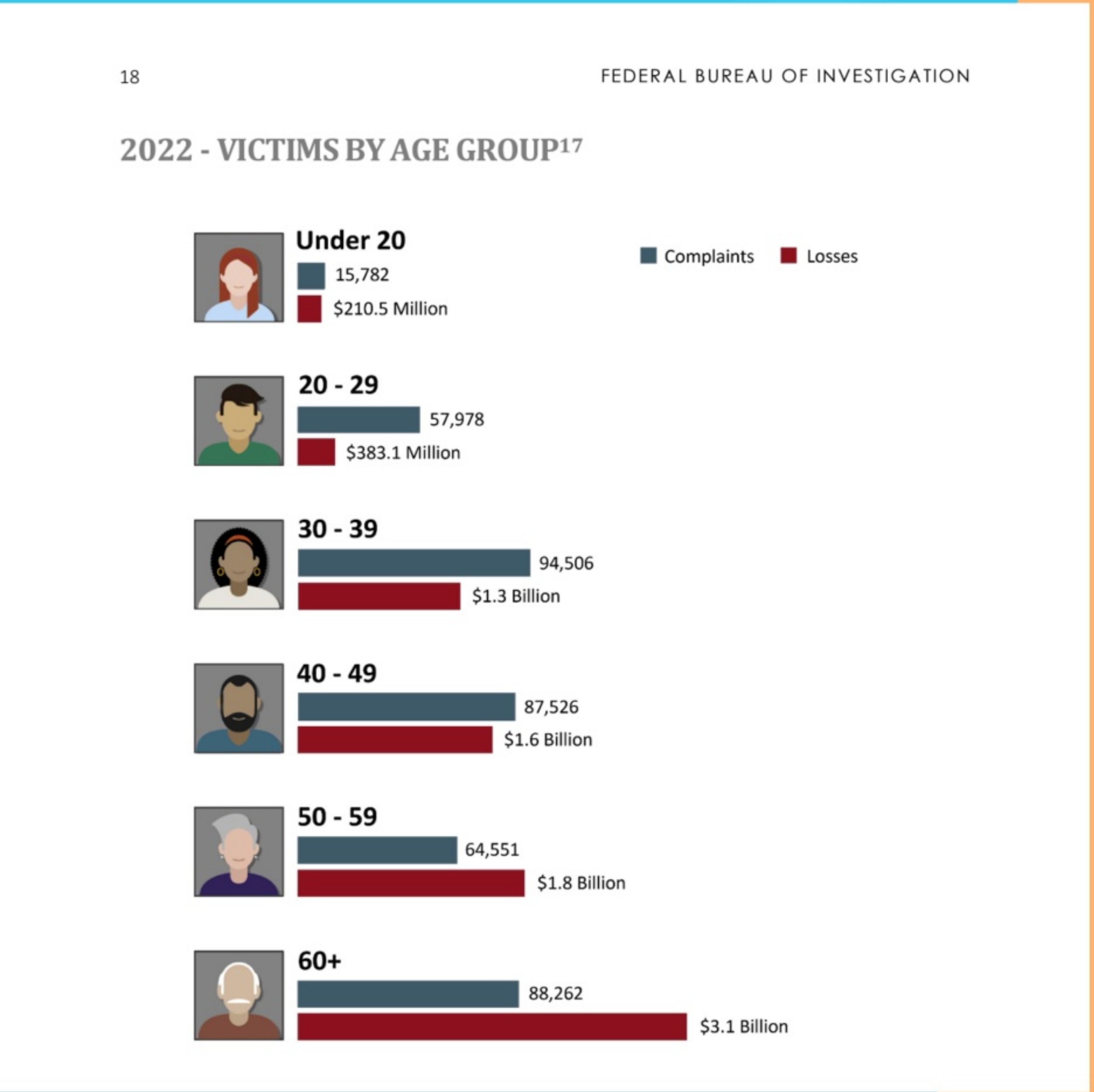
Cyber crime as defined

There are many definitions of cyber crime...

"Any illegal activity for which a computer is used as its primary means of commission, transmission, or storage" and is divided into 3 categories:

- *crimes in which the computing device is the target*
- *crimes in which the computer is the weapon*
- *crimes in which the computer is used as an accessory to a crime (DOJ)*

"Cyber risk is business risk" and "cybersecurity is national security," (FBI, 2022 IC3 report).

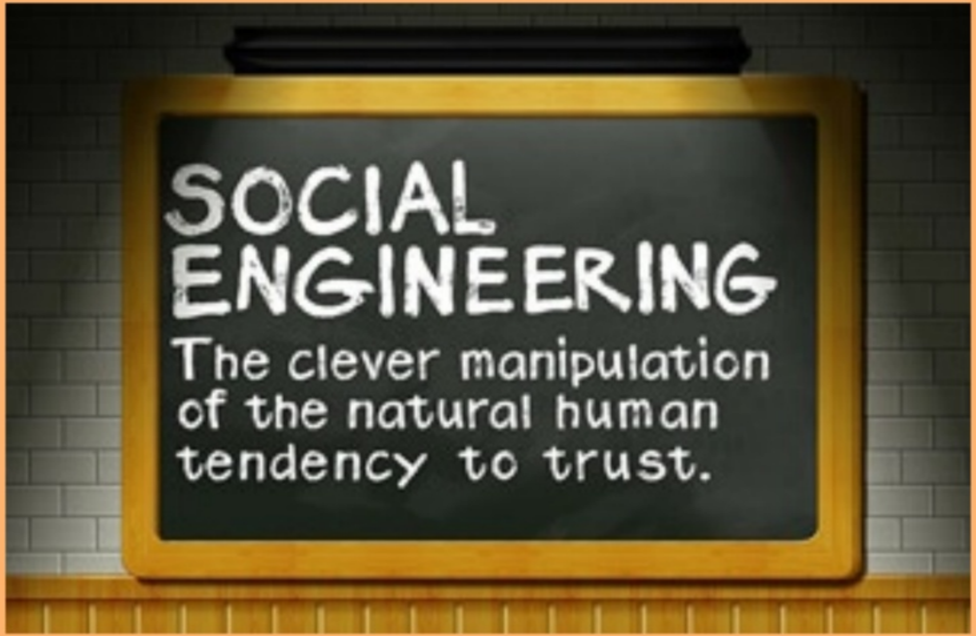


18 FEDERAL BUREAU OF INVESTIGATION

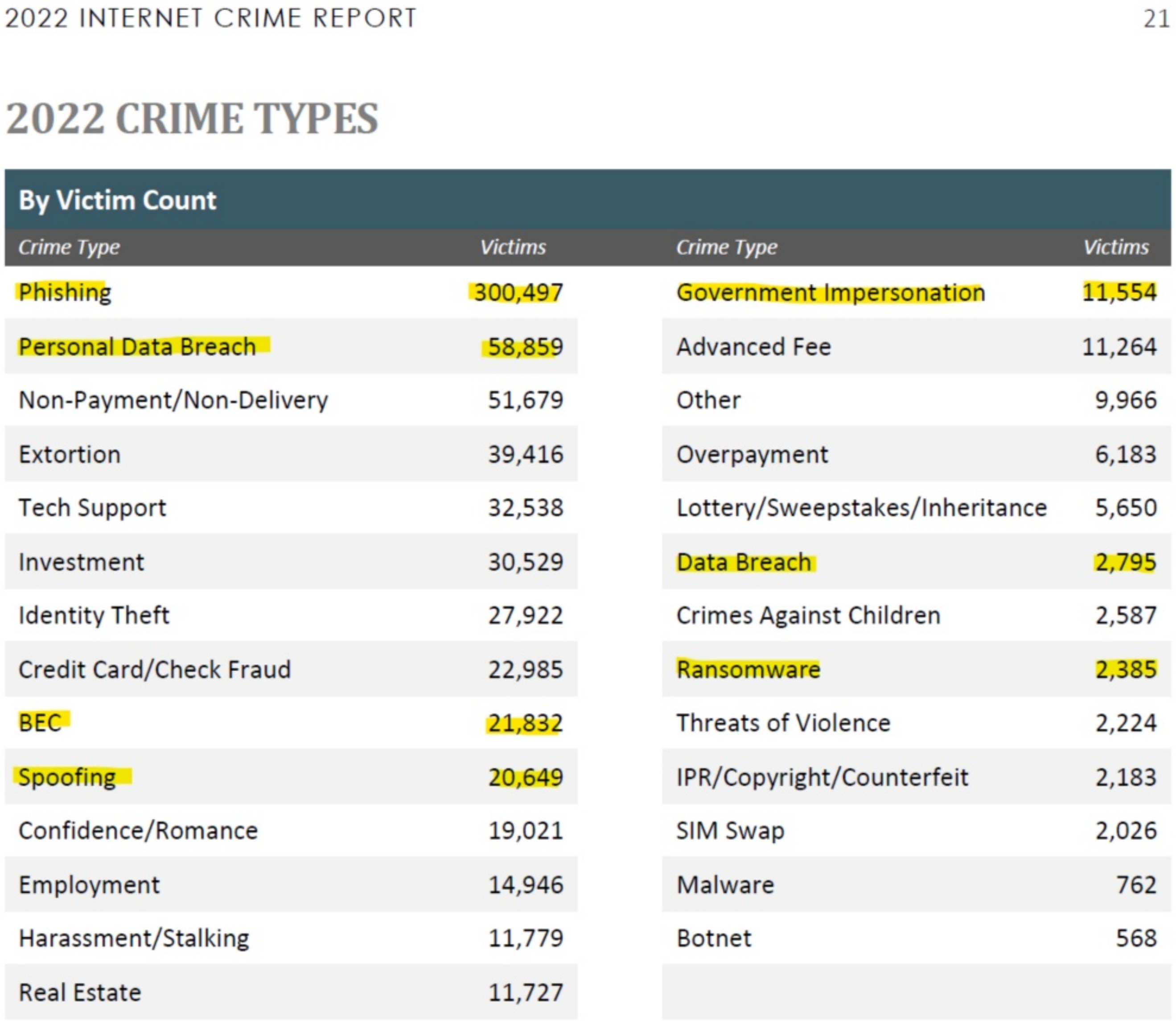
2022 - VICTIMS BY AGE GROUP[17]

Cyber crime can happen at home and at work

eCrime is launched and executed using Social Engineering which is:



SOCIAL ENGINEERING
The clever manipulation of the natural human tendency to trust.



2022 INTERNET CRIME REPORT 21

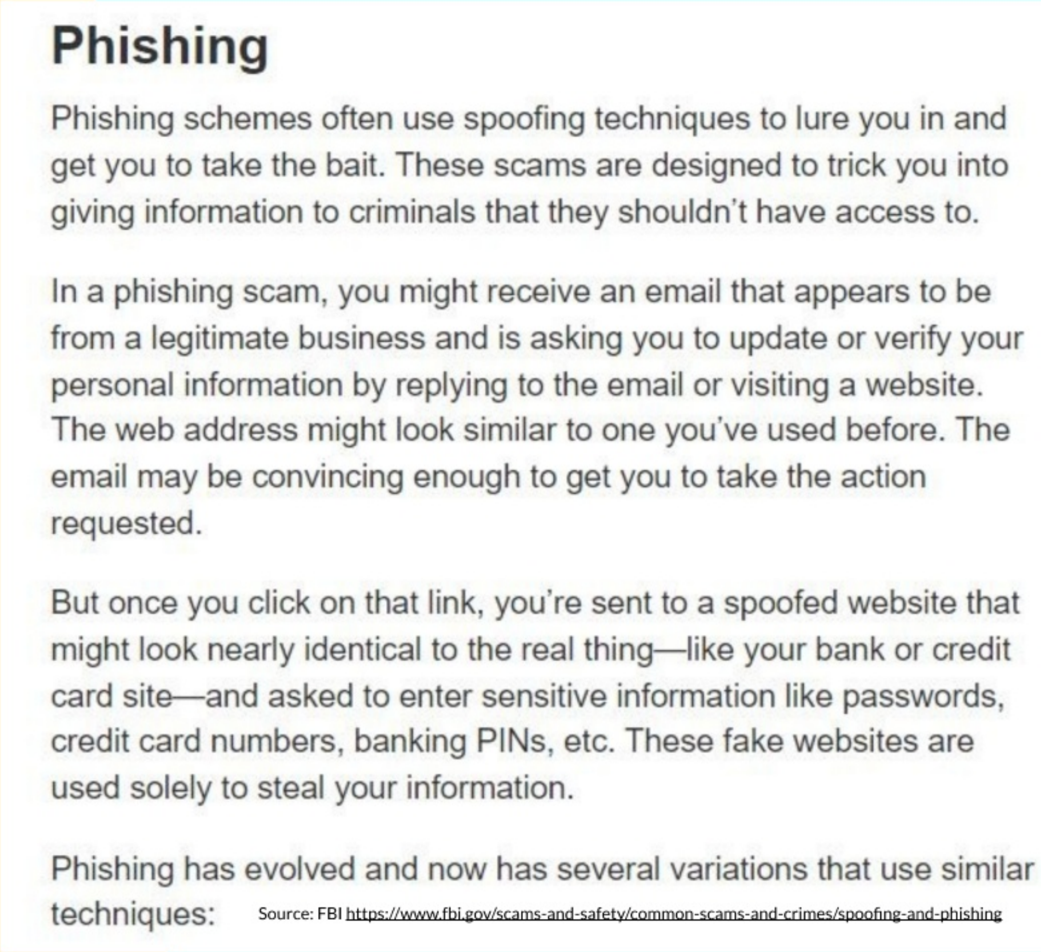
2022 CRIME TYPES

By Victim Count

Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		

Phishing is just Digital Fishing

The FBI lists Phishing as using Spoofing techniques to lure us in to taking an action(s).



Phishing

Phishing schemes often use spoofing techniques to lure you in and get you to take the bait. These scams are designed to trick you into giving information to criminals that they shouldn't have access to.

In a phishing scam, you might receive an email that appears to be from a legitimate business and is asking you to update or verify your personal information by replying to the email or visiting a website. The web address might look similar to one you've used before. The email may be convincing enough to get you to take the action requested.

But once you click on that link, you're sent to a spoofed website that might look nearly identical to the real thing—like your bank or credit card site—and asked to enter sensitive information like passwords, credit card numbers, banking PINs, etc. These fake websites are used solely to steal your information.

Phishing has evolved and now has several variations that use similar techniques:

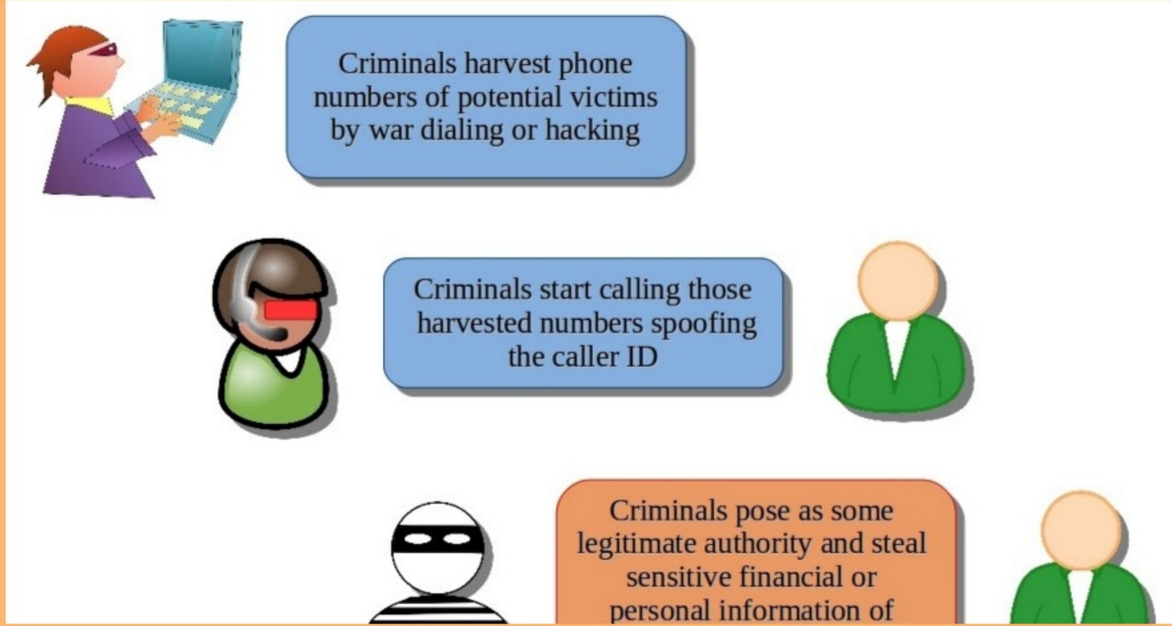
Source: FBI https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing

Vishing...say what?!

Vishing are scams that happen over the phone, voice email, VoIP (voice over internet protocol) calls.

The ultimate goal for both phishing and vishing is the same—**to exploit victims in order to profit in some way,** whether financially or otherwise.

Source: Panda Security



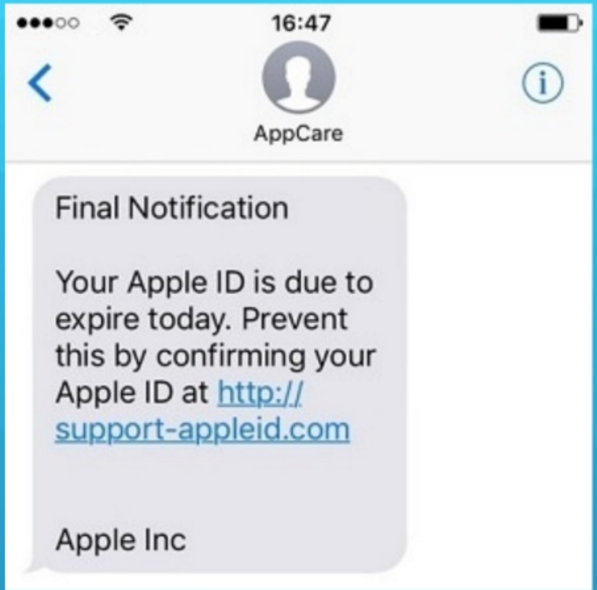
Criminals harvest phone numbers of potential victims by war dialing or hacking

Criminals start calling those harvested numbers spoofing the caller ID

Criminals pose as some legitimate authority and steal sensitive financial or personal information of

SMiShing

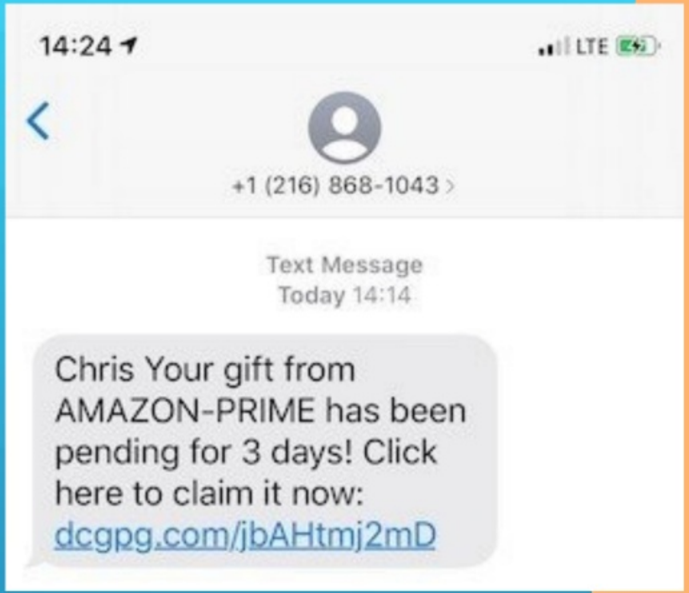
SMS scams (a.k.a Smishing) is a quick, easy, and very popular tactic used today that targets mobile devices.



Final Notification

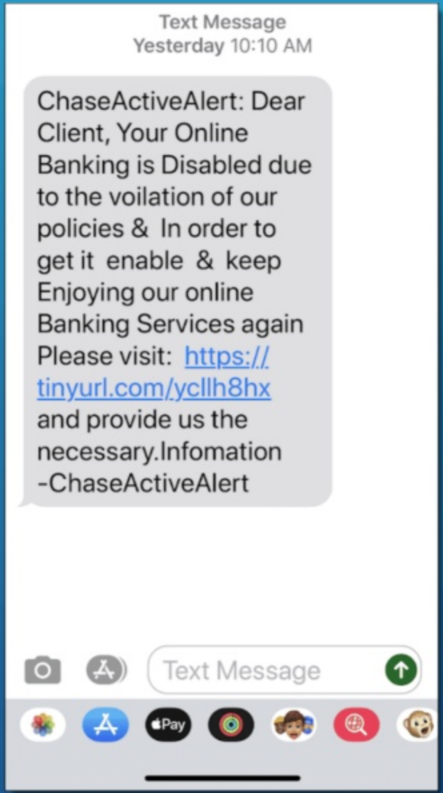
Your Apple ID is due to expire today. Prevent this by confirming your Apple ID at http://support-appleid.com

Apple Inc

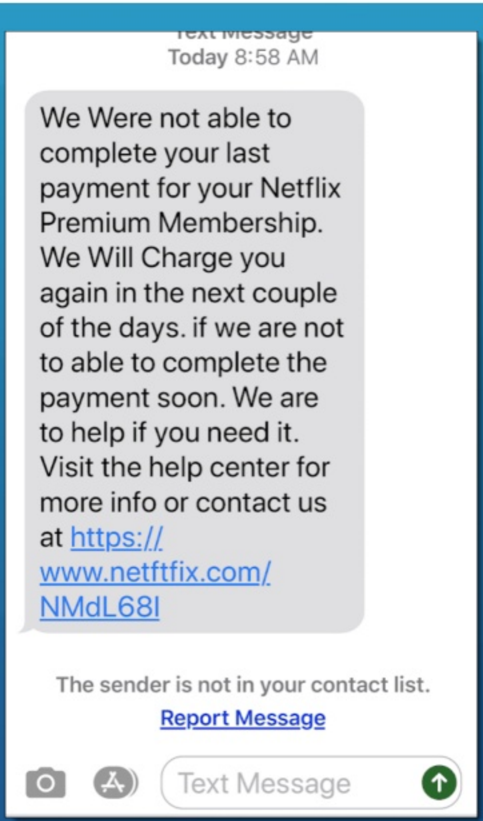


Text Message
Today 14:14

Chris Your gift from AMAZON-PRIME has been pending for 3 days! Click here to claim it now: dcgpg.com/jbAHtmj2mD

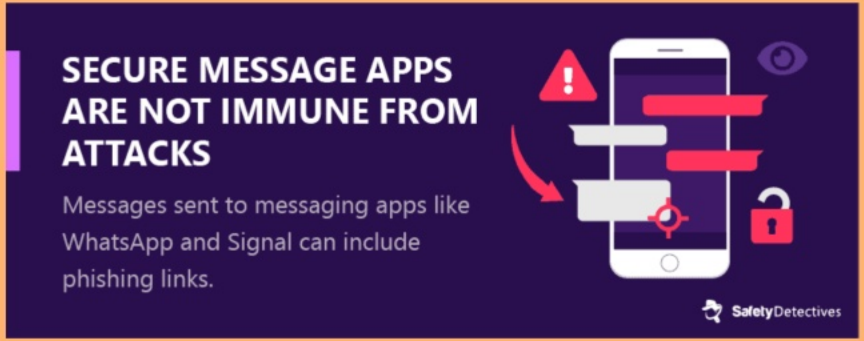

Text Message
Yesterday 10:10 AM

ChaseActiveAlert: Dear Client, Your Online Banking is Disabled due to the voilation of our policies & In order to get it enable & keep Enjoying our online Banking Services again Please visit: https://tinyurl.com/ycllh8hx and provide us the necessary.Infomation -ChaseActiveAlert


Text Message
Today 8:58 AM

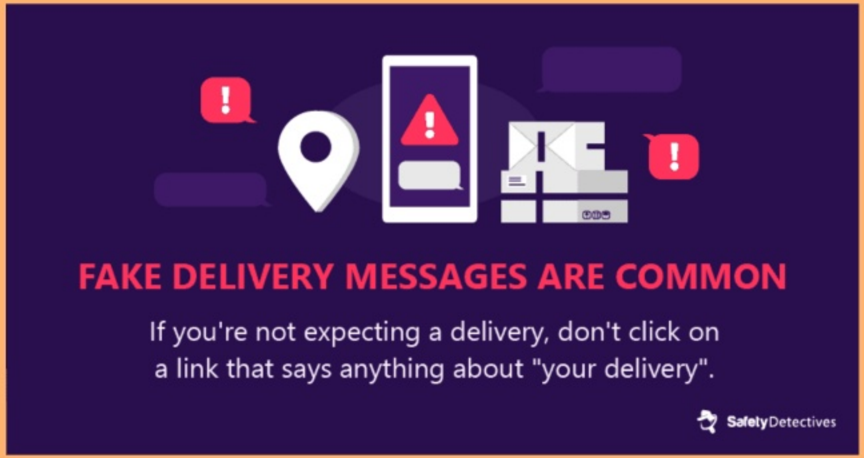
We Were not able to complete your last payment for your Netflix Premium Membership. We Will Charge you again in the next couple of the days. if we are not to able to complete the payment soon. We are to help if you need it. Visit the help center for more info or contact us at https://www.netftfix.com/NMdL68I

The sender is not in your contact list.
Report Message



SECURE MESSAGE APPS ARE NOT IMMUNE FROM ATTACKS

Messages sent to messaging apps like WhatsApp and Signal can include phishing links.



FAKE DELIVERY MESSAGES ARE COMMON

If you're not expecting a delivery, don't click on a link that says anything about "your delivery".

Who is doing this?

The Unusual Suspects

Cyber threats, methods and motivations

BAE SYSTEMS
INSPIRED WORK
7'0"
6'0"
5'0"
4'0"

The Mule

The Mule is motivated by greed or desperation. They are the final link in the chain – and most vulnerable to arrest.

The Professional

They work a 9-to-5 day job that looks legitimate – but the reality couldn't be further from the truth.

The Nation State Actor

The Nation State Actor has a 'Licence to Hack' – and they use it to target their adversaries.

The Activist

Whatever their cause, it's a burning one. The Activist's tactics cross the line from legitimate protest into criminality.

The Getaway

The Getaway is too young to go to jail: even if they're caught, they're unlikely to get more than a slap on the wrist.

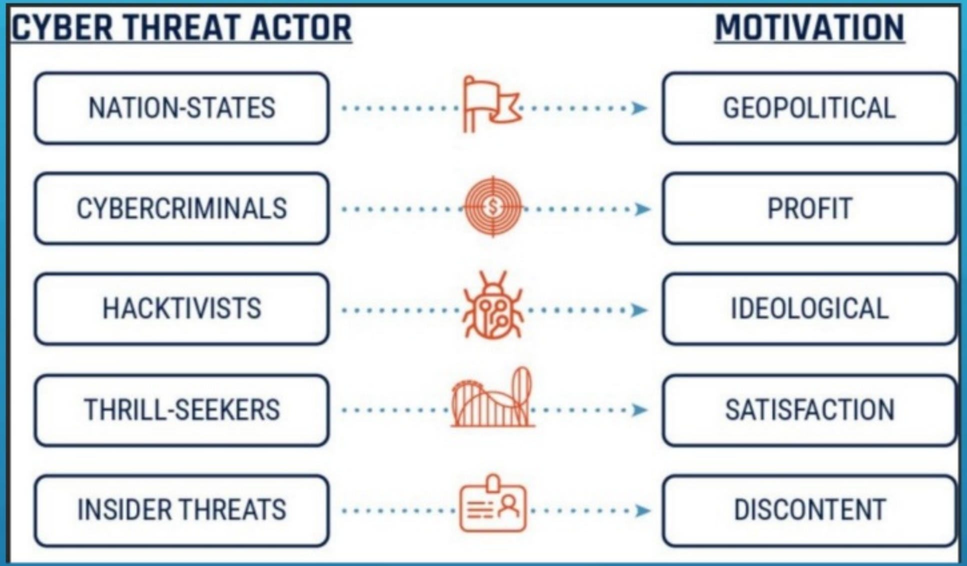
The Insider

They're fed up, blackmailed, or just being really helpful. Your business' defences are wide open to the Insider.

BAEsystems.com/unusualsuspects

It's not just security. It's defence.

Counties face constant cyber threats both External and possibly Internal sources.



CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

Source: The Cyber Story. https://thecyberstory.wordpress.com/2020/04/27/cyber-threat-actors-know-your-enemy/

Do Vendors pose a potential cyber risk?

6 common signs* of Business Email Compromise

Time sensitive request

A covert request

Grammatical errors & spelling mistakes (less common)

Direct messages from Vendors

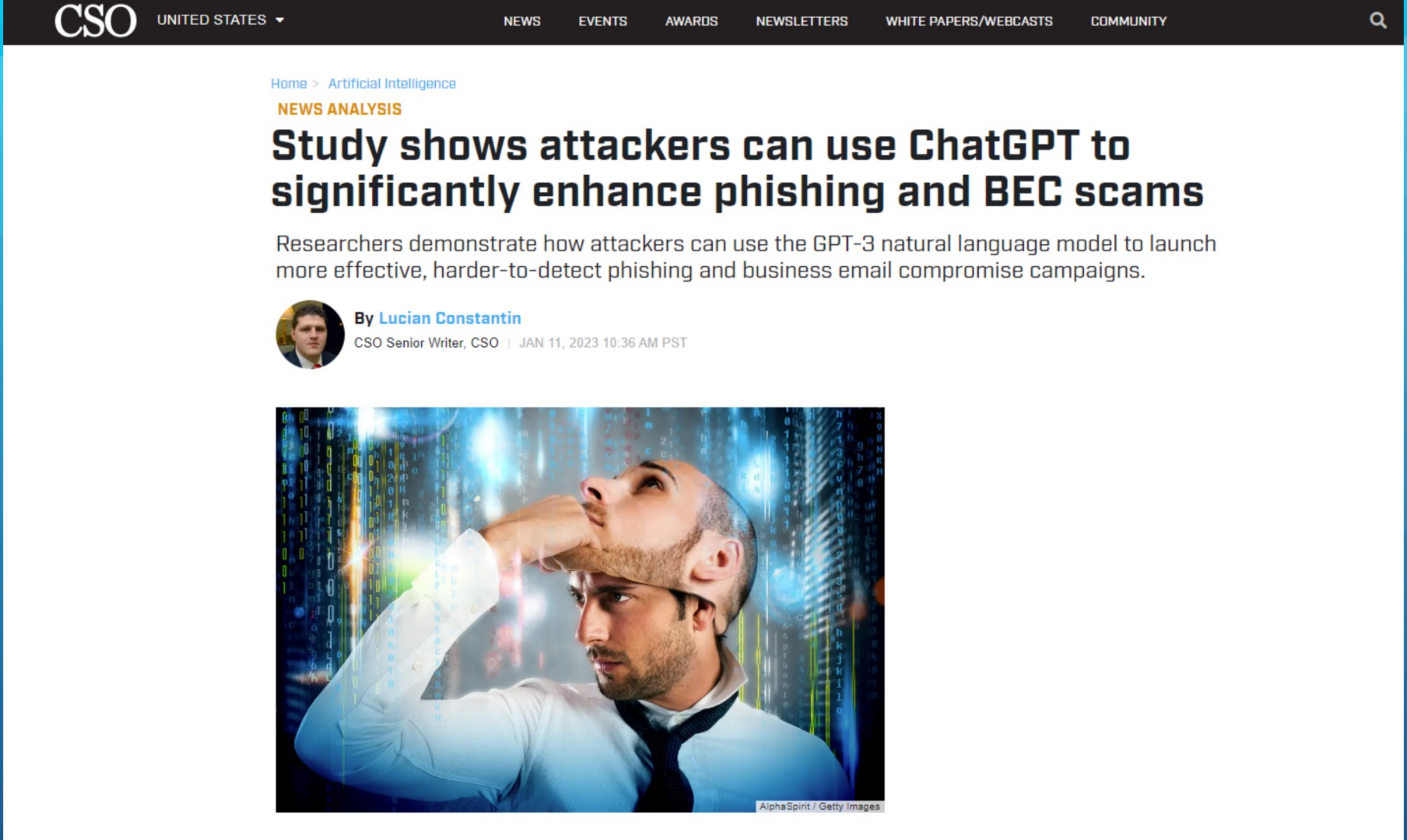
Personal information or money is required immediately

Messages from Personal Email and Mobile

Types

Show me the Money

** Hackers are constantly evolving their tactics and these common signs will change - do not rely on solely. **



Home > Artificial Intelligence

NEWS ANALYSIS

Study shows attackers can use ChatGPT to significantly enhance phishing and BEC scams

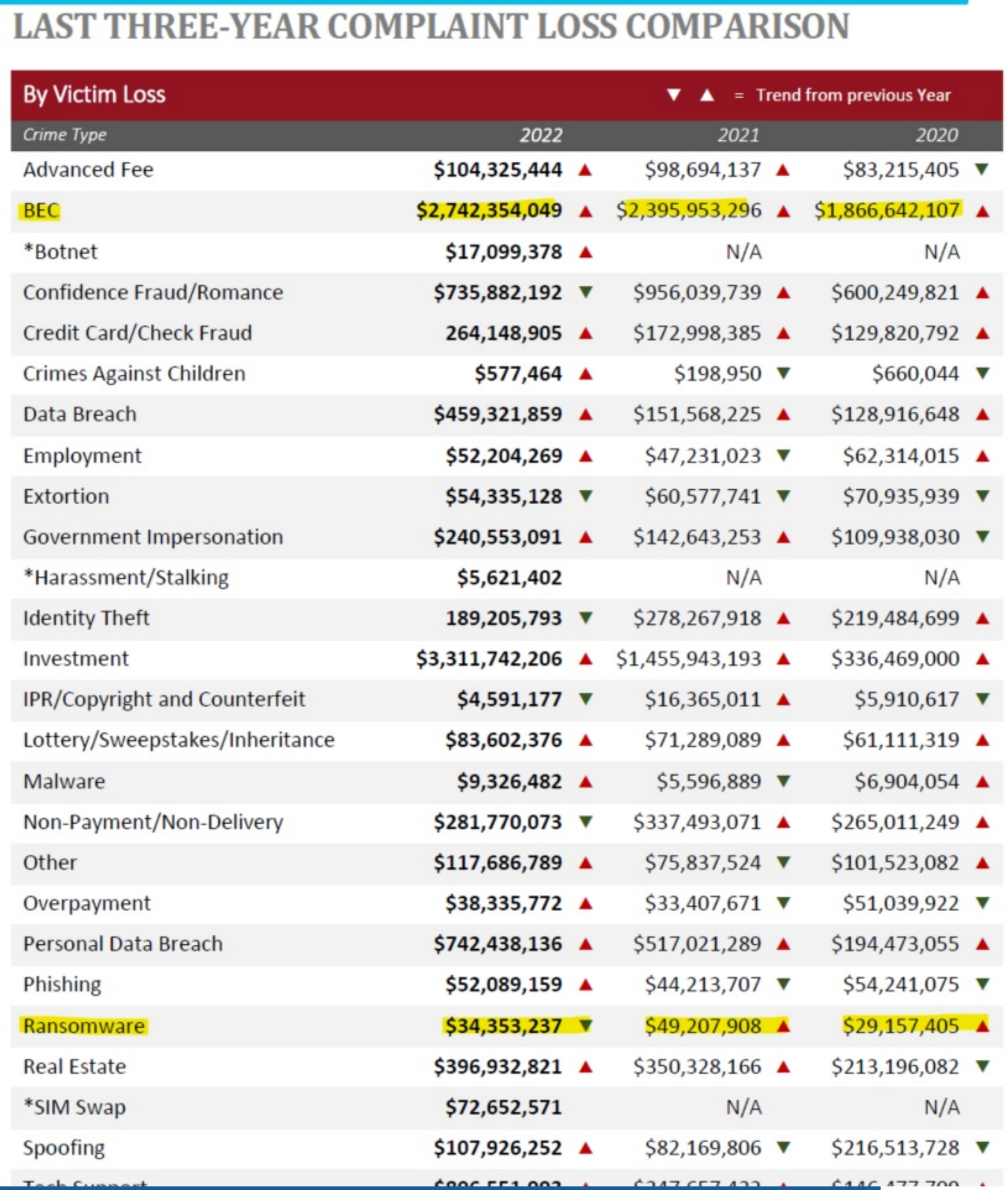
Researchers demonstrate how attackers can use the GPT-3 natural language model to launch more effective, harder-to-detect phishing and business email compromise campaigns.

By Lucian Constantin

CSO Senior Writer, CSO | JAN 11, 2023 10:36 AM PST

AlphaSpirit / Getty Images

Source: Oliver Muenchow, Lucy. 01.29.21 https://youtu.be/j7PrXMnSW3Y



LAST THREE-YEAR COMPLAINT LOSS COMPARISON

By Victim Loss ▼ ▲ = Trend from previous Year

Crime Type	*2022*	*2021*	*2020*
Advanced Fee	**$104,325,444** ▲	$98,694,137 ▲	$83,215,405 ▼
BEC	**$2,742,354,049** ▲	$2,395,953,296 ▲	$1,866,642,107 ▲
*Botnet	**$17,099,378** ▲	N/A	N/A
Confidence Fraud/Romance	**$735,882,192** ▼	$956,039,739 ▲	$600,249,821 ▲
Credit Card/Check Fraud	**264,148,905** ▲	$172,998,385 ▲	$129,820,792 ▲
Crimes Against Children	**$577,464** ▲	$198,950 ▼	$660,044 ▼
Data Breach	**$459,321,859** ▲	$151,568,225 ▲	$128,916,648 ▲
Employment	**$52,204,269** ▲	$47,231,023 ▼	$62,314,015 ▲
Extortion	**$54,335,128** ▼	$60,577,741 ▼	$70,935,939 ▼
Government Impersonation	**$240,553,091** ▲	$142,643,253 ▲	$109,938,030 ▼
*Harassment/Stalking	**$5,621,402**	N/A	N/A
Identity Theft	**189,205,793** ▼	$278,267,918 ▲	$219,484,699 ▲
Investment	**$3,311,742,206** ▲	$1,455,943,193 ▲	$336,469,000 ▲
IPR/Copyright and Counterfeit	**$4,591,177** ▼	$16,365,011 ▲	$5,910,617 ▼
Lottery/Sweepstakes/Inheritance	**$83,602,376** ▲	$71,289,089 ▲	$61,111,319 ▲
Malware	**$9,326,482** ▲	$5,596,889 ▼	$6,904,054 ▲
Non-Payment/Non-Delivery	**$281,770,073** ▼	$337,493,071 ▲	$265,011,249 ▲
Other	**$117,686,789** ▲	$75,837,524 ▼	$101,523,082 ▲
Overpayment	**$38,335,772** ▲	$33,407,671 ▼	$51,039,922 ▼
Personal Data Breach	**$742,438,136** ▲	$517,021,289 ▲	$194,473,055 ▲
Phishing	**$52,089,159** ▲	$44,213,707 ▼	$54,241,075 ▼
Ransomware	**$34,353,237** ▼	$49,207,908 ▲	$29,157,405 ▲
Real Estate	**$396,932,821** ▲	$350,328,166 ▲	$213,196,082 ▼
*SIM Swap	**$72,652,571**	N/A	N/A
Spoofing	**$107,926,252** ▲	$82,169,806 ▼	$216,513,728 ▼
Tech Support	**$806,551,993** ▲	$347,657,432 ▲	$146,477,709 ▲

The Data says...

While Ransomware dominates the headlines, it is Business Email Compromise (BEC) that is the second most costliest cause of Victim Financial Loss, per the FBI's 2022 IC3 Report.

- BEC is easier to execute than most Ransomware
- BEC is embarrassing versus Ransomware is an existential crisis
- Most business/organizations don't report BEC
- BEC is about a mass attack, unlike Ransomware which is highly targeted

How do we mitigate BEC and possibly prevent it?

We will never be able to eliminate all cyber risk. As our world becomes more and more digitized, we will have to learn to adapt to a cybersecurity mindset at home and on the job.

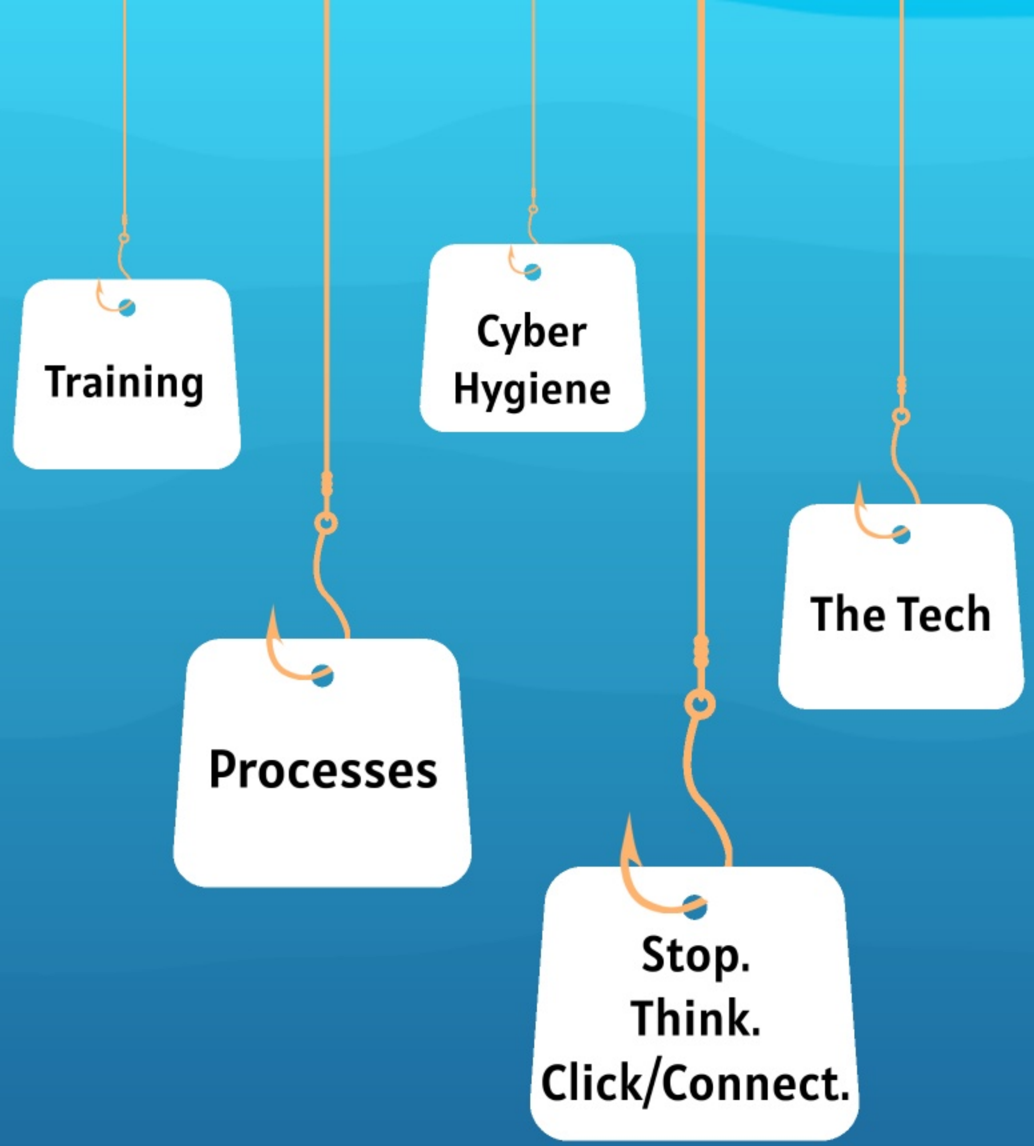
Traditional Mindset

Trust but verify.

Ronald Reagan

Cybersecurity Mindset

and then



Training

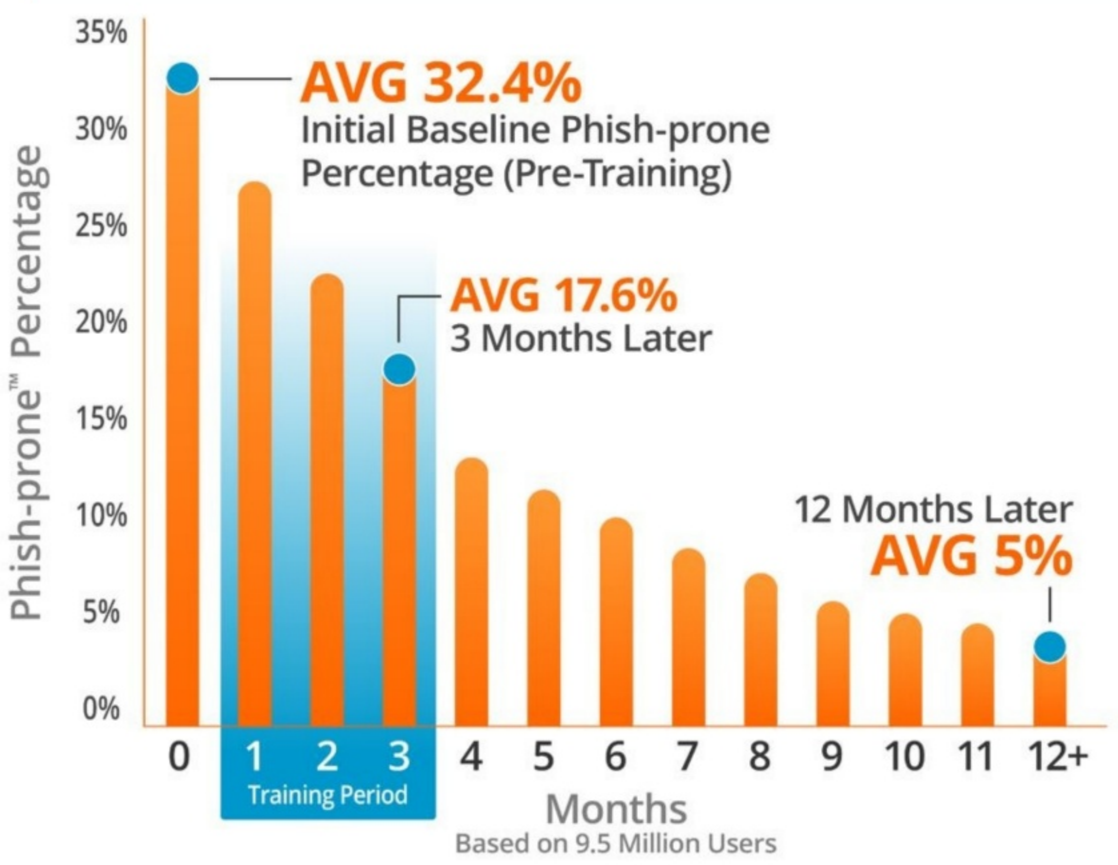
Cyber Hygiene

Processes

The Tech

Stop. Think. Click/Connect.

1. We have to accept that Humans are the weakest link and that we **(counties and employees)** are a target for cyber criminals.
2. Consistent and timely training on phishing email simulations, social engineering and cyber hygiene.
3. Utilize phishing email tools like Phish Alert Button or other email plug-ins to report fraudulent emails to IT.
4. Build and maintain a culture of security awareness that leads to having human firewalls.

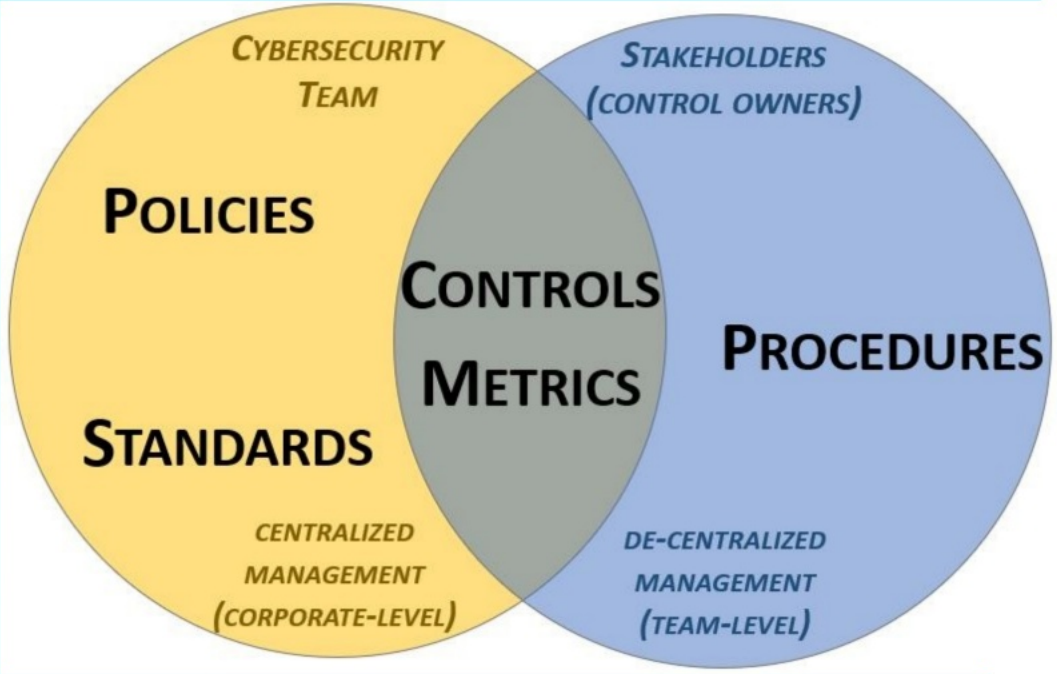


Source: 2022 KnowBe4 Phishing by Industry Benchmarking Report

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.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
CYBERSECURITY AWARENESS MONTH 2022
SEE YOURSELF IN CYBER

Every county is different and your procedures and controls may vary.



Cybersecurity Team
Stakeholders (control owners)
Policies
Controls
Metrics
Procedures
Standards
centralized management (corporate-level)
de-centralized management (team-level)

Source: Compliance Forge: https://www.complianceforge.com/faq/word-crimes/policy-vs-standard-vs-control-vs-procedure

Review your technology vendor contracts

Types of Security for Paper Records

- Locked storage areas
- Fire and flood protection
- Secured storage facilities
- Off-site copies and backups

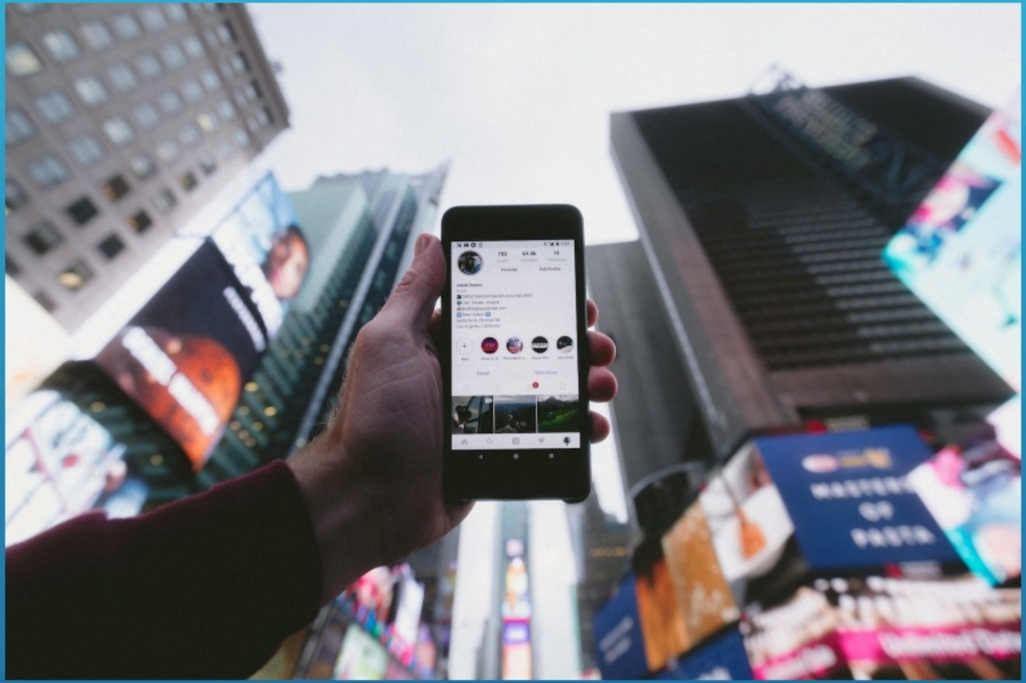
Types of Security for Electronic Records

- Document redaction
- Access control lists
- File encryption (at rest and in-transit)
- BEC policy for your office
- Vendor audits

The Human Factor

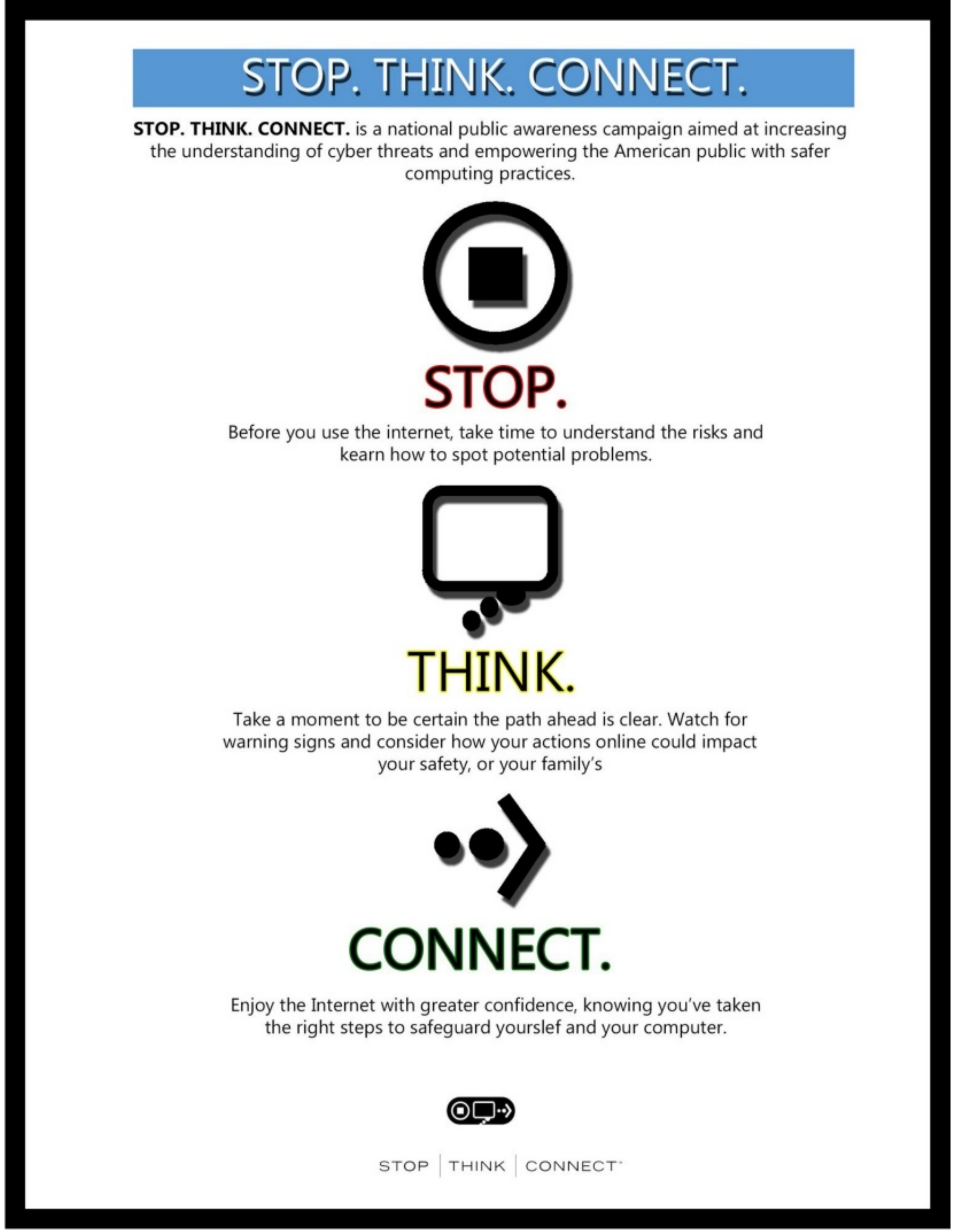
Things to consider about YOUR OFFICE:

- Separation of duties
- Be mindful of what information you share online or on social media
- Build relationships with your vendors, get to know them and make them part of your process
- Stop. Think before you Click or Connect.
- Require strong and unique passwords
- Establish what can be done via **Email** versus what must be done in **Person**



At Home,
At Work,
While on Mobile

Businesses, organizations, governmental entities and public education are joining the movement



STOP. THINK. CONNECT.

STOP. THINK. CONNECT. is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public with safer computing practices.

STOP.

Before you use the internet, take time to understand the risks and kearn how to spot potential problems.

THINK.

Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's

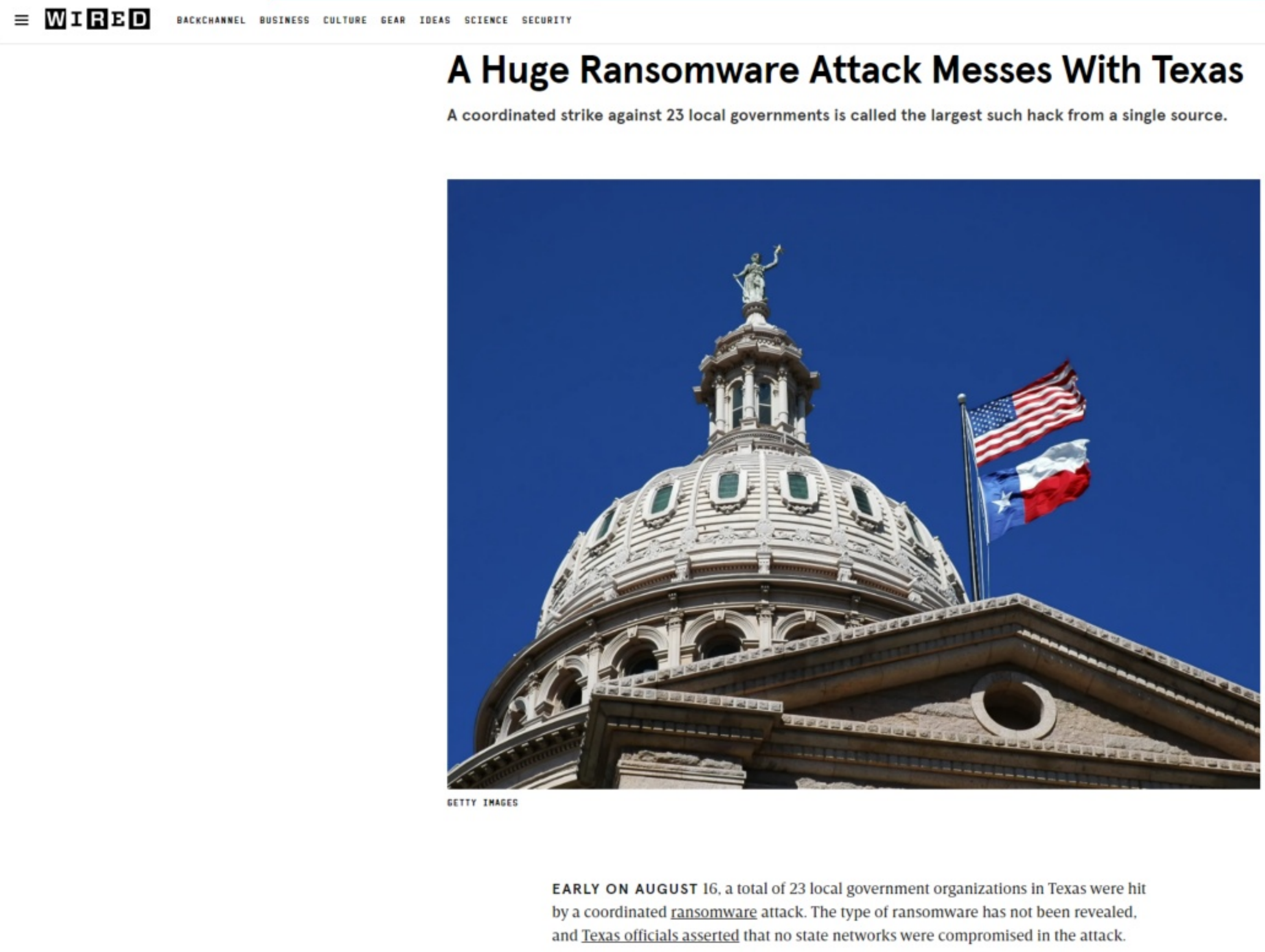
CONNECT.

Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourslef and your computer.

STOP | THINK | CONNECT™

Cyber hits close to home…

- August 16, 2019 - large scale ransomware attack
- Attack began in the middle of the night
- Attack caused heavy disruption to various local governments
- Later discovered that attack launched by threat actor group, REvil
- REvil allegedly gained access via TSM Consulting Services Inc. (vendor) screen-sharing and remote admin services to access networks

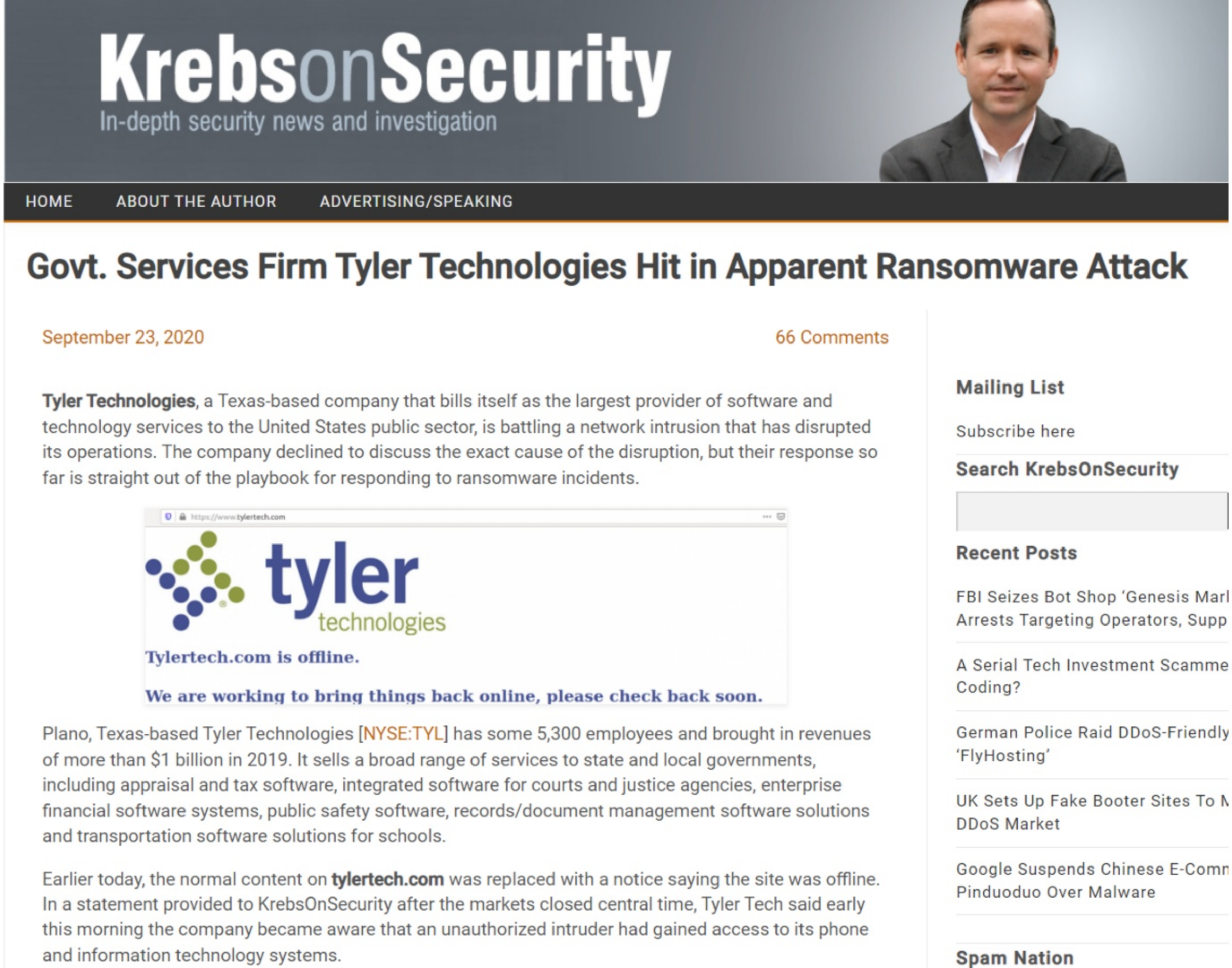


A Huge Ransomware Attack Messes With Texas

A coordinated strike against 23 local governments is called the largest such hack from a single source.

GETTY IMAGES

EARLY ON AUGUST 16, a total of 23 local government organizations in Texas were hit by a coordinated ransomware attack. The type of ransomware has not been revealed, and Texas officials asserted that no state networks were compromised in the attack.



KrebsonSecurity
In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Govt. Services Firm Tyler Technologies Hit in Apparent Ransomware Attack

September 23, 2020 66 Comments

Tyler Technologies, a Texas-based company that bills itself as the largest provider of software and technology services to the United States public sector, is battling a network intrusion that has disrupted its operations. The company declined to discuss the exact cause of the disruption, but their response so far is straight out of the playbook for responding to ransomware incidents.

https://www.tylertech.com

tyler technologies

Tylertech.com is offline.

We are working to bring things back online, please check back soon.

Plano, Texas-based Tyler Technologies [NYSE:TYL] has some 5,300 employees and brought in revenues of more than $1 billion in 2019. It sells a broad range of services to state and local governments, including appraisal and tax software, integrated software for courts and justice agencies, enterprise financial software systems, public safety software, records/document management software solutions and transportation software solutions for schools.

Earlier today, the normal content on **tylertech.com** was replaced with a notice saying the site was offline. In a statement provided to KrebsOnSecurity after the markets closed central time, Tyler Tech said early this morning the company became aware that an unauthorized intruder had gained access to its phone and information technology systems.

Mailing List

Subscribe here

Search KrebsOnSecurity

Recent Posts

FBI Seizes Bot Shop 'Genesis Marl Arrests Targeting Operators, Supp

A Serial Tech Investment Scamme Coding?

German Police Raid DDoS-Friendly 'FlyHosting'

UK Sets Up Fake Booter Sites To M DDoS Market

Google Suspends Chinese E-Comn Pinduoduo Over Malware

Spam Nation

- RansomEXX suspected
- Same ransomware impacted Tx DOT
- Tyler paid and unspecified ransom to get the decryption key

BEC (eCrime) is about deception at its core.

Cybersecurity has to be a shared responsibility and not solely that of IT.

Some key resources:

- **eRiskHub** (login and password required) for Cyber members
- **NACo Cyber Guide for County Leaders**
- **StopRansomware** - www.cisa.gov/stopransomware
- **Internet Complaint Center (IC3) -** www.ic3.gov
- **National Cybersecurity Alliance -** www.staysafeonline.org
- **Cybersecurity Risk Consultant**
- **Risk Management Consultant**
- **TAC RMP cyber workshop**

Robert Ruiz
Associate Director
rruiz@county.org
512-779-3621