Cybersecurity Awareness

Eric Kehmeier / November 2nd, 2022

Integrated Business Technologies
1800 South Elm Pl., Suite 200 / Broken Arrow, OK
918.770.8738 / www.IBTsupport.com

WHY WE'RE HERE

- My mission when I started as an MSP
- My experience with Ransomware
- My new mission has been to bring security focus to the owners and staff of all small businesses who CAN avoid getting breached.

AGENDA

- ❑ Evolution of Cybercrime – WHY this is happening
- ❑ Prime Targets – WHO it's happening to
- ❑ Threat Vectors – HOW the bad guys get in
- ❑ Your Role – WHAT you can do to protect yourself, your family and your employer
- ❑ Time to Shift – WHAT you need to win
- ❑ Resources – WHERE you can go to learn more

IBT

EVOLUTION OF CYBERCRIME

Why is this happening?

WHY – THE EVOLUTION OF CYBERCRIME

Payment systems*

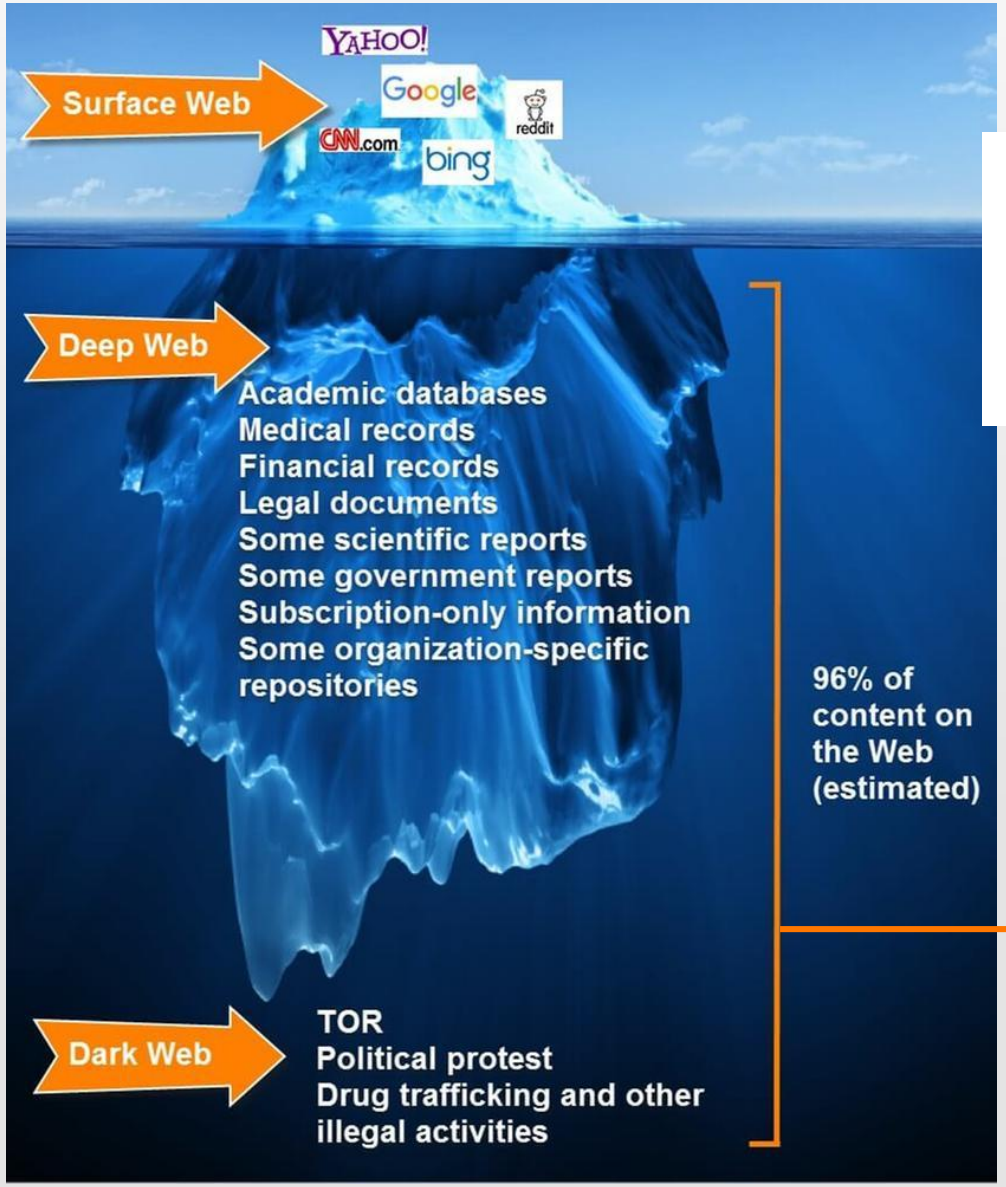
#	NAME	MARKET CAP	PRICE
1	BTC Bitcoin	1.04724416244e+11	$6117.67
2	ETH Ethereum	43575743019.4	$434.30
3	XRP Ripple	18177638381.9	$0.462982
4	BCH Bitcoin Cash	12160605068.9	$706.75

Job postings

Marketplaces

*Source: Coinmarketcap.com/currencies/icon 7-8-2018

CYBERCRIME ON THE DARK WEB



Stolen credentials are used to test for open door access into corporate networks

197 Days: the average length of time it takes for organizations to identify a data breach

19 Minutes to Escalation: Russian Hackers Move the Fastest

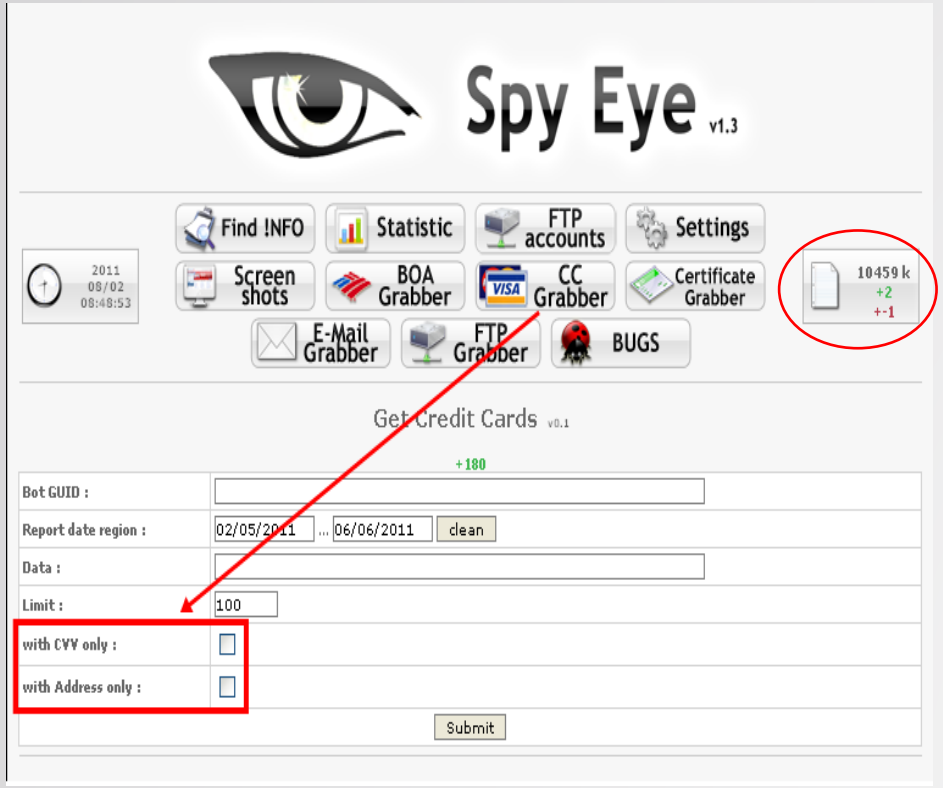
New data from CrowdStrike's incident investigations in 2018 uncover just how quickly nation-state hackers from Russia, North Korea, China, and Iran pivot from patient zero in a target organization.

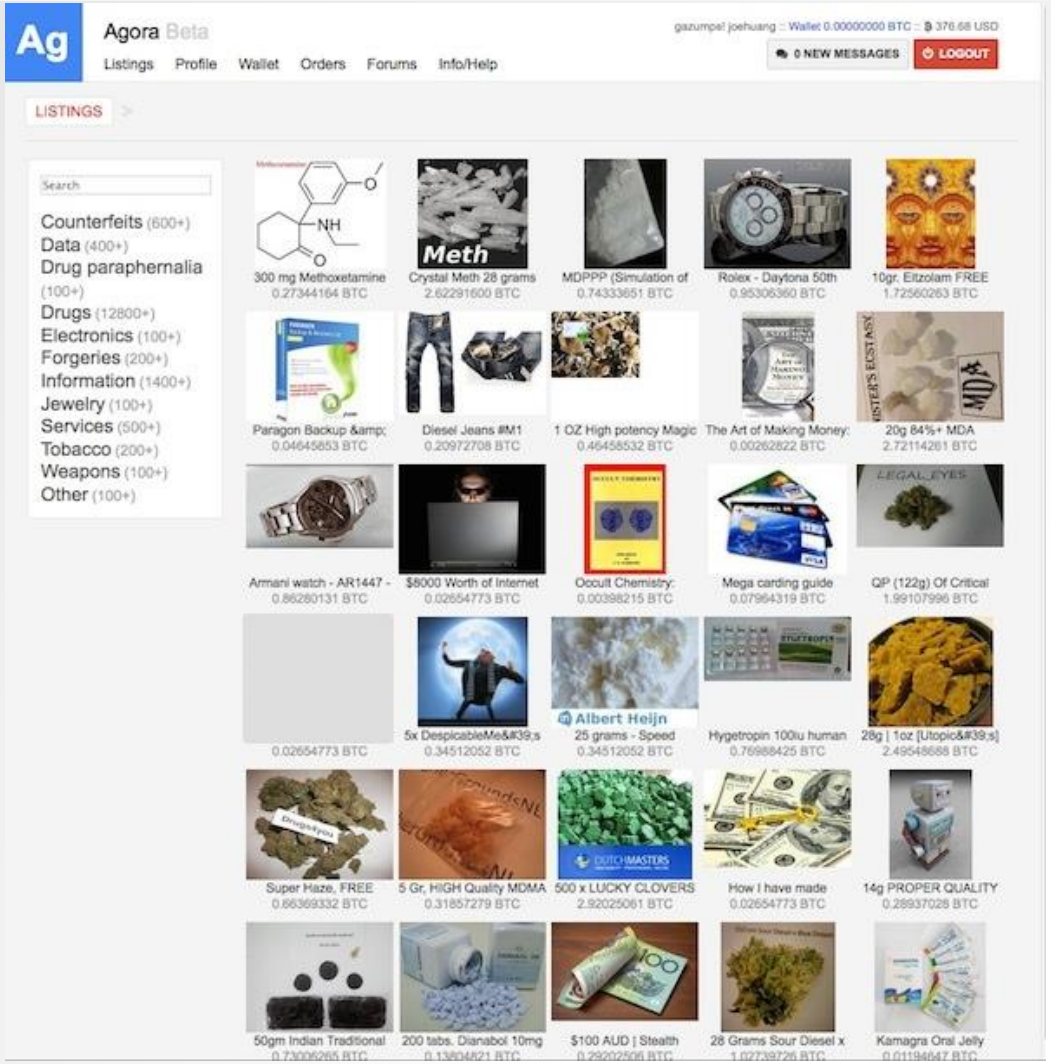
News

By KELLY JACKSON HIGGINS Executive Editor at Dark Reading, 2/19/2019

Stolen Credentials Are Sold Here

CYBERCRIME ONLINE SHOPPING…

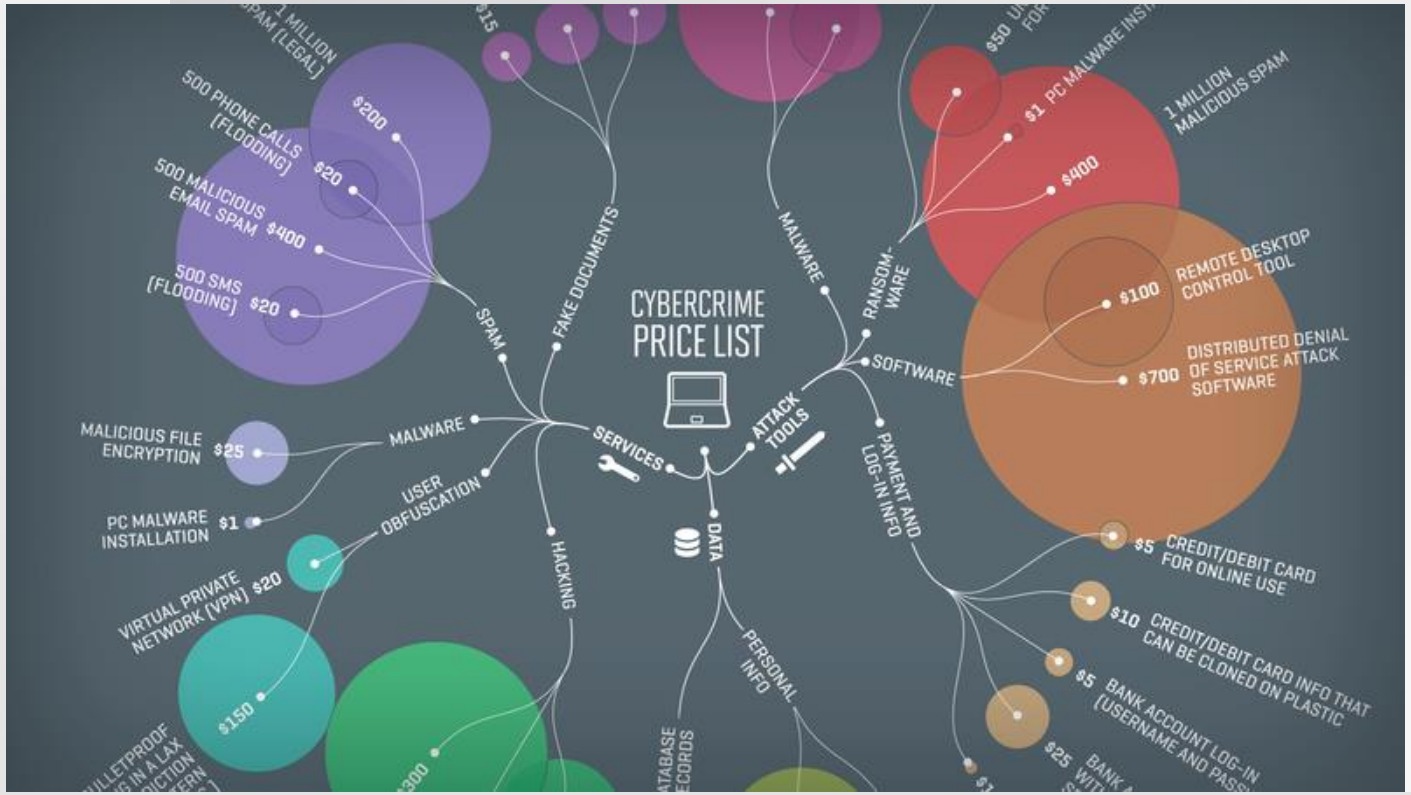




CYBER CRIME IS COMPETITIVE!

PHISHING

Lucrative Payoff

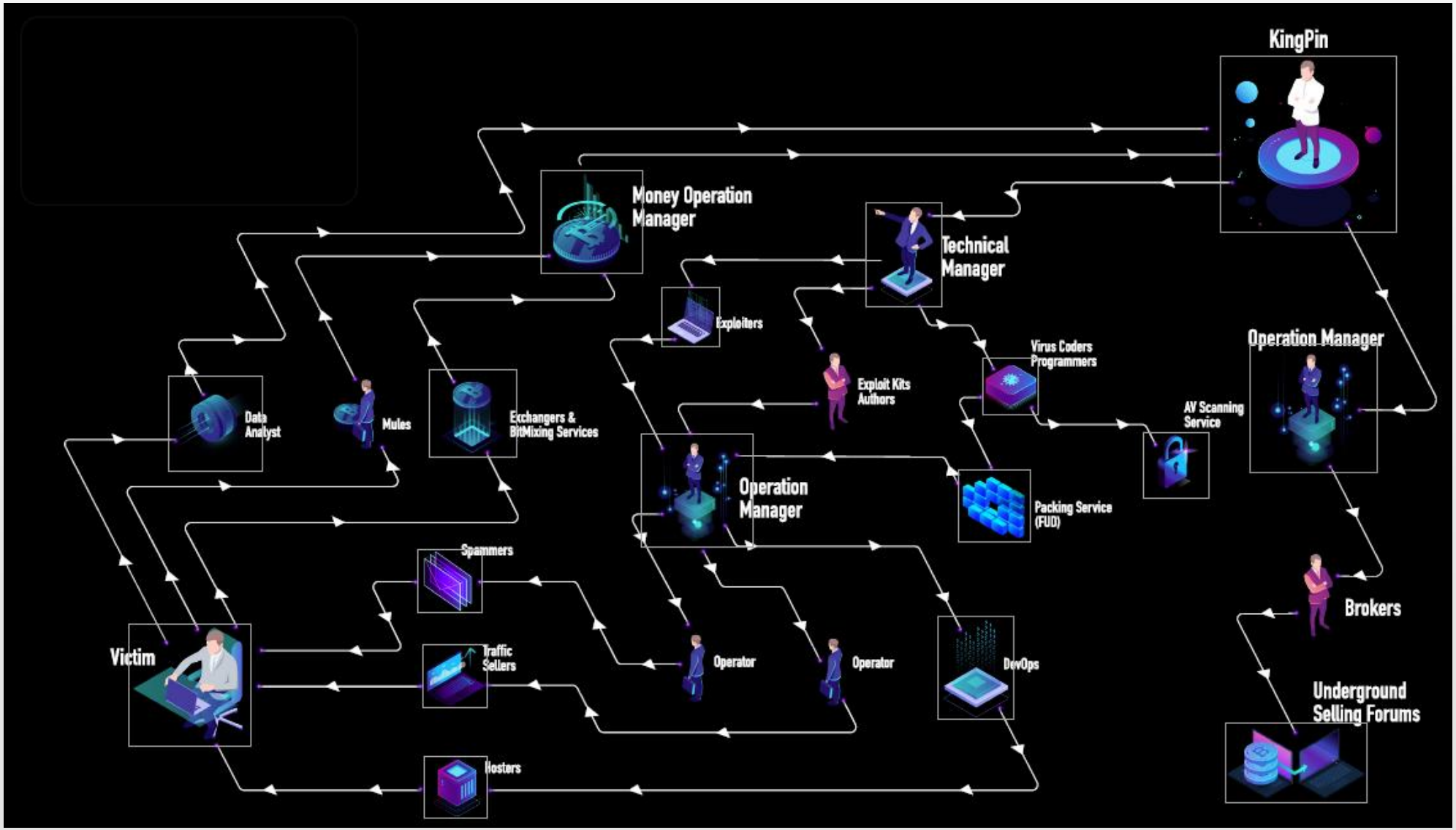


CYBERCRIME PRICE LIST

ATTACK TOOLS	MALWARE	$200	REMOTE ACCESS TROJAN
		$50	PASSWORD STEALER
	RANSOMWARE	200	SOPHISTICATED LICENSE FOR WIDESPREAD ATTACKS
		$50	UNSOPHISTICATED LICENSE FOR TARGETED ATTACKS
		$1	PC MALWARE INSTALLATION
		$400	1 MILLION MALICIOUS SPAM
	SOFTWARE	$100	REMOTE DESKTOP CONTROL TOOL
		$700	DISTRIBUTED DENIAL OF SERVICE ATTACK SOFTWARE
	PAYMENT & LOG-IN INFO	$5	CREDIT/DEBIT CARD FOR ONLINE USE
		$10	CREDIT/DEBIT CARD INFO THAT CAN BE CLONED ON PLASTIC
		$5	BANK ACCOUNT LOG-IN (USERNAME AND PASSWORD)
		$25	BANK ACCOUNT LOG-IN WITH ACCESS TO EMAIL, SECURITY ANSWERS, ETC.
		$1	EXISTING PAYPAL ACCOUNT
DATA	PERSONAL INFORMATION	$3	SOCIAL SECURITY AND DATE OF BIRTH VERIFICATION
		$150	CREDIT REPORT 750+ CREDIT SCORE
	DATABASE RECORDS	$25	1 MILLION COMPROMISED EMAIL/PASSWORDS
SERVICES	HACKING	$100	EMAIL ACCOUNT
		$100	SOCIAL MEDIA ACCOUNT
		$300	CMS WEBSITE (WORDPRESS, ETC.)
	USER OBFUSCATION	$150	BULLETPROOF HOSTING IN A LAX JURISDICTION (CHINA, EASTERN EUROPE, ETC.)
		$20	VIRTUAL PRIVATE NETWORK (VPN)
	MALWARE	$1	PC MALWARE INSTALLATION
		$25	MALICIOUS FILE ENCRYPTION
	SPAM	$20	500 SMS (FLOODING)
		$400	500 MALICIOUS EMAIL SPAM
		$20	500 PHONE CALLS (FLOODING)
		$200	1 MILLION EMAIL SPAM (LEGAL)
	FAKE DOCUMENTS	$25	DIGITAL COPY OF FAKE CREDIT/DEBIT CARD
		$25	DIGITAL COPY OF FAKE DRIVER'S LICENSE OR PASSPORT
		$15	DIGITAL COPY OF FAKE UTILITY BILL OR SOCIAL SECURITY CARD

FORTUNE MAGAZINE
SOURCE: RECORDED FUTURE

WHAT ORGANIZED CRIME LOOKS LIKE



Source: Check Point Research, RSA presentation 2019

IBT

PRIME TARGETS

Who is this happening to?


THE HOME DEPOT


Wendy's


ebay

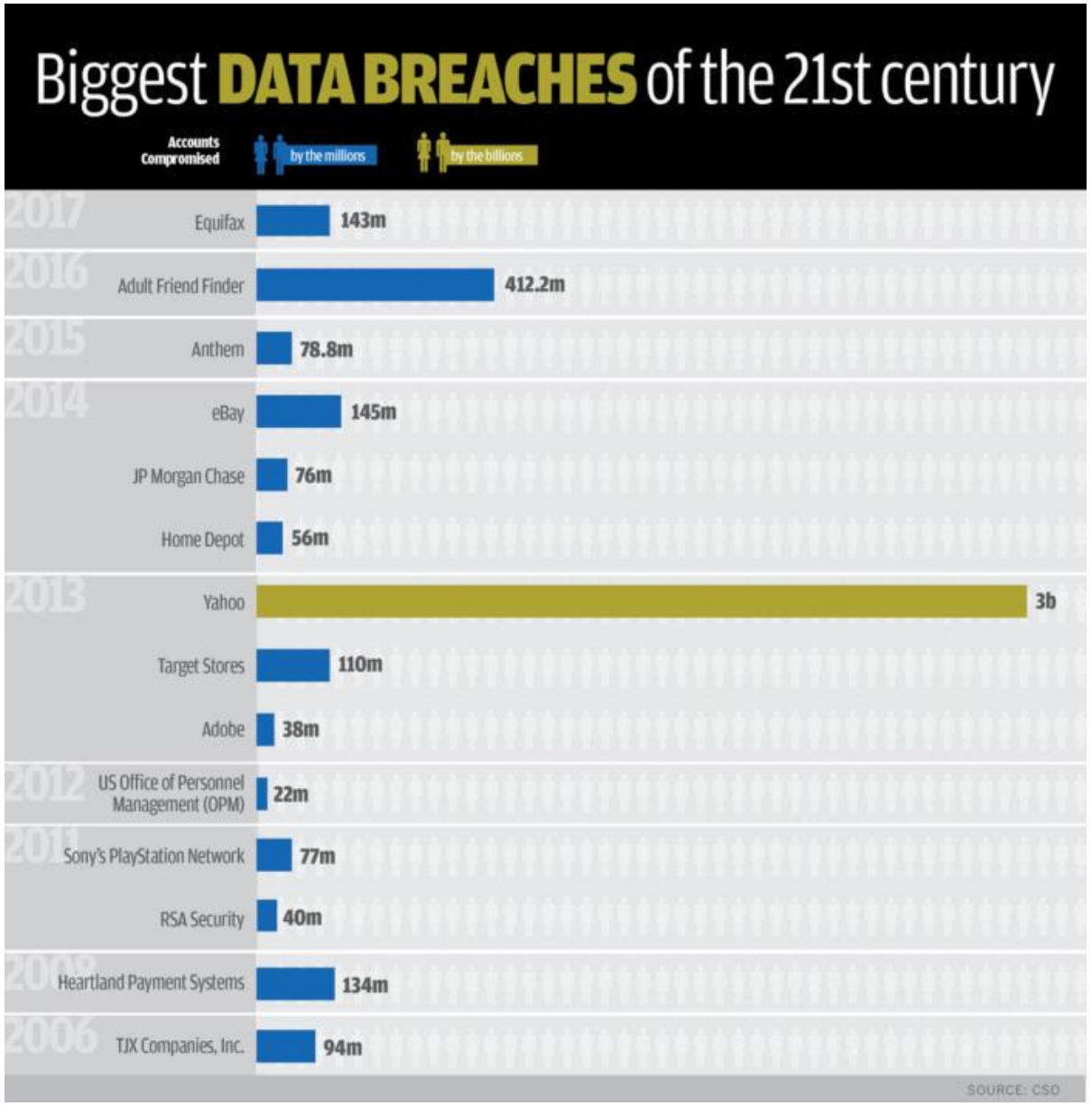

CHIPOTLE
MEXICAN GRILL

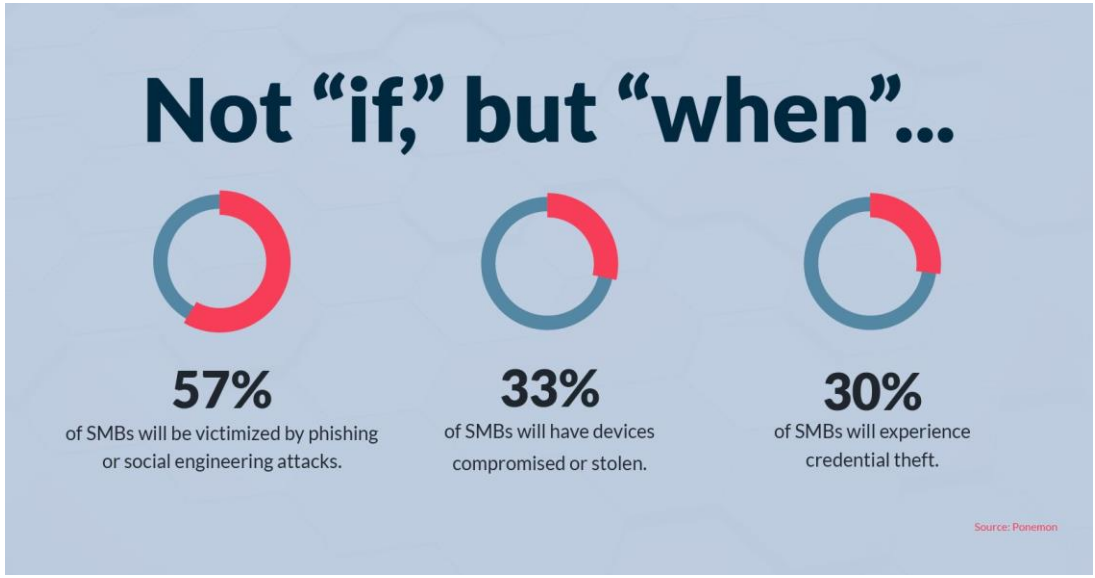

WHOLE FOODS
MARKET


Marriott
HOTELS • RESORTS • SUITES


Anthem


EQUIFAX





Will you be prepared?

WHY SMALL BUSINESSES ARE PRIME TARGETS

MALICIOUS EMAIL PER USER BY ORGANIZATION SIZE (YEAR)

ORGANIZATION SIZE	USERS TARGETED (1 IN)
1-250	6
251-500	6
501-1000	4
1001-1500	7
1501-2500	4
2501+	11

Source: Symantec 2019 Internet Threat Report

- ❑ Budget – SMB's spend less than 10% of their annual budget on IT (including support). They can't afford a $40,000 firewall and CISO on staff.
- ❑ Low IT skill level or no support unless something breaks
- ❑ Aging equipment and unpatched devices
- ❑ Owners wear many hats and don't focus on security
- ❑ SMB's don't believe it will happen to them
- ❑ SMB"s believe their data is not valuable
- ❑ SMB's far behind Enterprise in educating employees

Source: Verizon 2018 DBIR Report

IBT

THREAT VECTORS

How the bad guys get in

PHISHING - HOW IT WORKS

1. You inadvertently download a file with a spy-agent attached.
   How?
   a) Opening an email attachment with a hidden payload.
   b) Visiting an infected website via link from an email or just normal web browsing.

2. The agent sits dormant on your PC or Mac undetected by Malware/Virus scanning tools. This is called a Zero Day infection.

"In 2019, it is estimated that a business will fall victim to a Ransomware attack every 14 seconds." Cybersecurity Ventures, 2018

IBT

RANSOMWARE

- Reported by Unit 42, a cyber forensic and reporting entity of Palo Alto Networks: As of Summer of 2021 – the average ransomware payment demand has hit a new record high of $570,000.
- 2020's average was $312,000, a 171% growth in just a year – meaning it is working.
- Quadruple extortion is the newest trend amongst ransomware groups, coming in 4 different forms:

Average Ransomware Payment Hits $570,000 in H1 2021

A new report finds ransomware gangs now bundle extortion methods to make victims pay up after an attack.

August 09, 2021

#1 = Encryption, in which victims pay to regain access to scrambled data and compromised systems

#2 = Public Disclosure, in which attackers release sensitive information if ransom isn't paid

#3 = Denial of service (DoS), in which ransomware gangs launch DoS attacks to shut down a victim's public websites.

#4 = Harassment, in which attackers contact a victim's customers, business partners, employees, and media to tell them an organization was hacked.

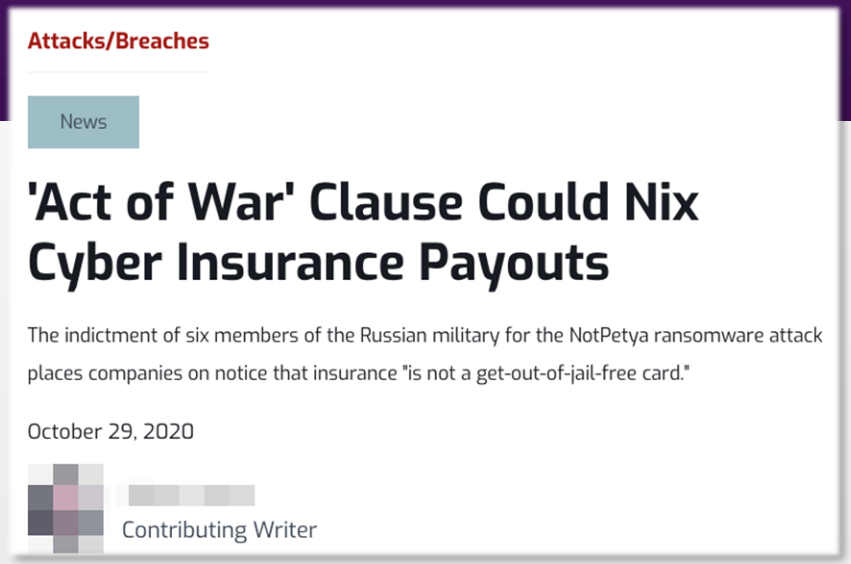
IBT

RANSOMWARE

- As a further form of persuasion, ransomware threat actors are more recently masking their identities, carrying out their attacks from various countries such as China or Russia.

- The reason for them doing this not only to mask their identity, but also coercing victims into paying that which cyber insurance firms are having tough times covering claims with due to “Act of War” clauses.

- Did you know you could be breaking the law if you pay a ransom, and those funds go to a terrorist group?



Attacks/Breaches

News

'Act of War' Clause Could Nix Cyber Insurance Payouts

The indictment of six members of the Russian military for the NotPetya ransomware attack places companies on notice that insurance "is not a get-out-of-jail-free card."

October 29, 2020

Contributing Writer

CYBERSECURITY

WSJ PRO CYBERSECURITY

WSJ PRO

Cyberattacks Complicate War Exclusions for Insurers

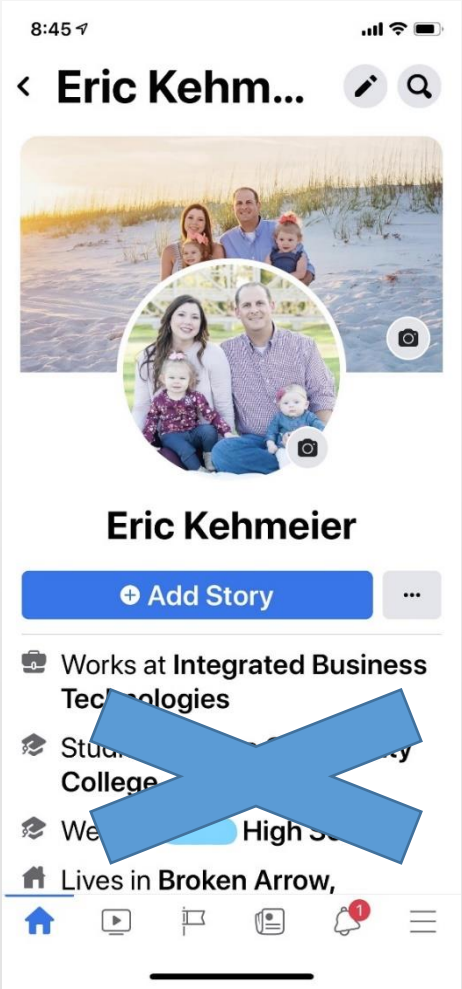
Insurance contracts typically exclude acts of war, but what is that exactly? With cybercrime, attacks often defy characterization.

SOCIAL ENGINEERING & PRETEXTING

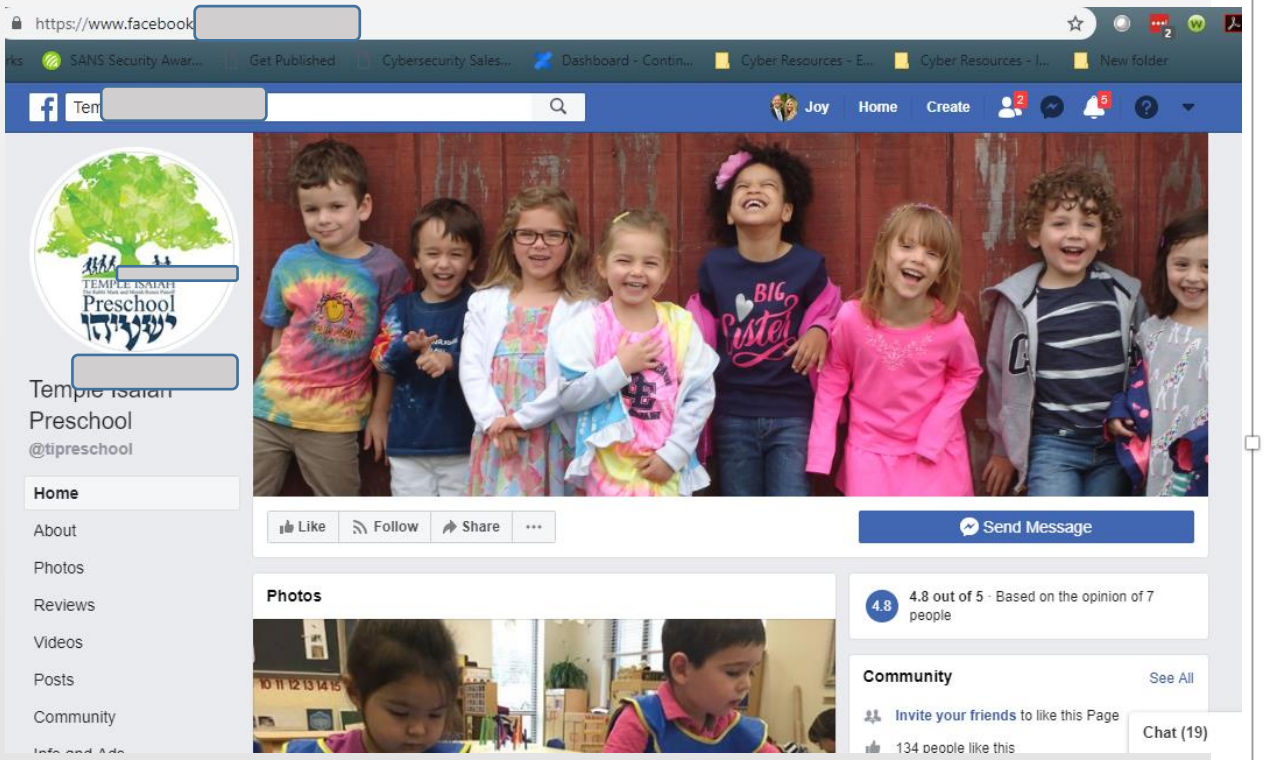
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

Social Engineering & Pretexting *do not* involve Malware at the outset. They are plotted and planned against specific victims.

As of 2018, global losses to BEC (business email compromise) have exceeded US$12 billion. ~Trend Micro, Year End Review 2018



SOCIAL ENGINEERING - PHONE CALLS



How to protect yourself from tech support scams

- If you receive an unsolicited email message or phone call that purports to be from Microsoft or another company asking that you to send personal information or click links, ignore or report the email, or hang up the phone. In general, unless you are absolutely sure you can trust the caller or the sender, do not share personal information, click links, or install applications when requested.

  Note that Microsoft does not send unsolicited email messages or make unsolicited phone calls to request for personal or financial information, or fix your computer.

- Do not trust unsolicited calls. Do not provide any personal information.

  Remember, Microsoft will never proactively reach out to you to provide unsolicited PC or technical support. Any communication we have with you must be initiated by you.

- Download software only from official vendor websites or the Microsoft Store. Be wary of downloading software from third-party sites, as some of them might have been modified without the author's knowledge to bundle support scam malware and other threats.

- Use Microsoft Edge when browsing the Internet. It blocks known support scam sites using Windows Defender SmartScreen (which is also used by Internet Explorer). Furthermore, Microsoft Edge can stop pop-up dialogue loops used by these sites.

  Don't call the number in the pop-ups. Microsoft's error and warning messages never include a phone number.

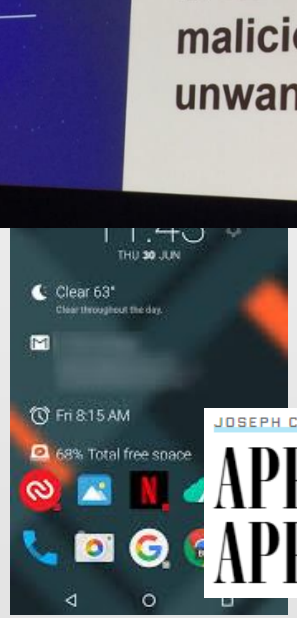
- Enable Windows Defender Antivirus on Windows 10. It detects and removes known support scam malware, such as SupportScam:AutoIt/Noland, SupportScam:JS/TechBrolo, SupportScam:MSIL/Hicurdismos, SupportScam:MSIL/Tifine.A, SupportScam:Win32/Cusax, SupportScam:Win32/Monitnev, and SupportScam:MSIL/Secupoint.A.

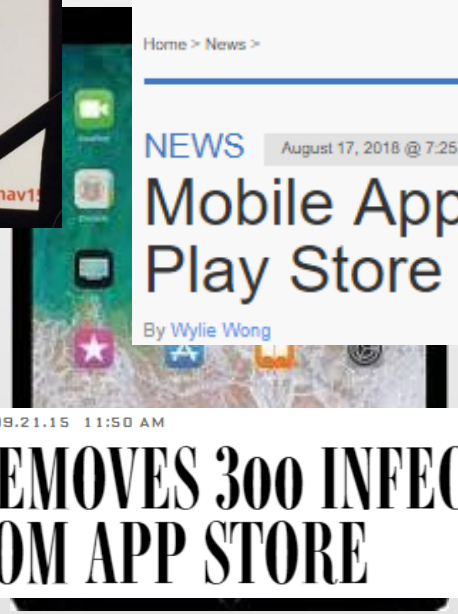
Reporting tech support scams

Help Microsoft stop scammers, whether they claim to be from Microsoft or from another tech company, by reporting tech support scams: **www.microsoft.com/reportascam**.

*Source: Microsoft website 6-28-2018

MOBILE DEVICES ARE FAIR GAME





SecurityIntelligence

NEWS 27 SERIES TOPICS INDUSTRIES

Home > News >

NEWS August 17, 2018 @ 7:25 AM

Mobile App Security Threat Forces Google Play Store to Remove 145 Android Apps

By Wylie Wong

JOSEPH COX SECURITY 09.21.15 11:50 AM

APPLE REMOVES 300 INFECTED APPS FROM APP STORE

SECURITY

Malicious iOS app popup windows c your Apple ID

It's simple to spoof a password request window, and nearly impossible and devs should watch out for.

By Brandon Vigliarolo | October 11, 2017, 8:50 AM PST

CYWARE My Feed All news Hacker News Newsletter Events

NEWS BY Categories Date Source

Google Play St

Recent History

September 24, 2019 | Malwa

- Recently, Google Play Store has been in the spotlight quite often for hosting malware-laced apps.
- Some of these apps have millions of downloads, posing a massive threat to a considerable chunk of Android users.

Context

Although Google lets in an app on the Play Store only after it satisfies a list of requirements, certain malicious apps seem to have discovered cracks to slip through. Sometimes, such apps record millions of downloads before they're discovered containing malware.

Google has been regularly weeding out malware-infected apps from the Play Store, but the openness of the platform is a roadblock in this battle.

Prominent incidents

Android users are told only to download apps from the official Play Store. Let's take a look at the recent instances of Google-approved apps sneaking in malware.

July 2019 - Around 205 malicious apps that were reported to have been downloaded more than 32 million times in July alone. These apps were found to contain malicious code that had the capabilities of stalkerware, backdoor, subscription scams, and more.

August 2019 - A popular PDF creator called CamScanner was discovered to contain a malicious module called 'Trojan-Dropper.AndroidOS.Necro.n'. The module was observed to show intrusive ads. After Kaspersky reported this to Google, the application was immediately removed.

September 2019 - This month witnessed the discovery of a new malware campaign to deliver the Joker Trojan. Google promptly removed the 24 apps that hid malicious code in the advertisement framework.

Google removed two adware apps, Sun Pro Beauty Camera and Funny Sweet

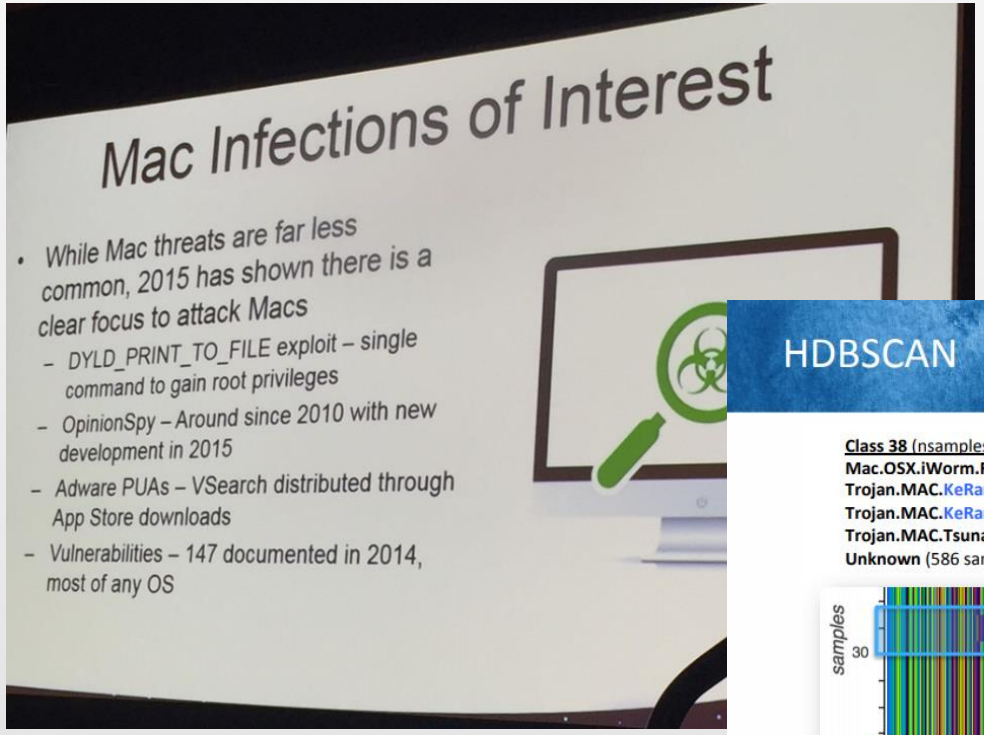
Just in September 2019, 25 malicious apps with 2.1 million downloads in total were observed serving random ads to generate revenue.

The takeaway

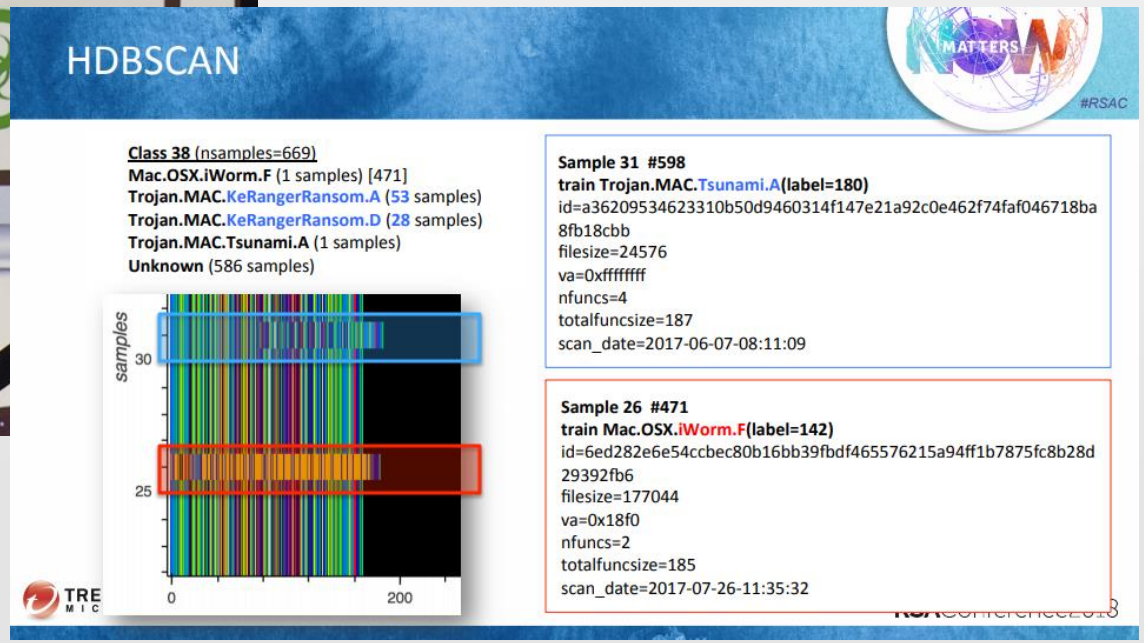
Google Play Store is still the safest place to download Android applications, but with so many incidents reported, users are advised to be on alert. No app is completely immune to being exploited for malicious purposes.

*Source: Webroot 2016, Verizon State of Security Report 2018,
http://fortune.com/2017/09/14/google-play-android-malware/
Wired online magazine https://www.wired.com/2015/09/apple-removes-300-infected-apps-app-store/
https://securityintelligence.com/news/mobile-app-security-threat-forces-google-play-store-to-remove-145-android-apps/

MACS ARE FAIR GAME




```
Cluster 2 (nsamples=668)
        KeRangerRansom.A (53 samples)
        KeRangerRansom.D (28 samples)
        Tsunami.A (1 samples)
        Unknown (586 samples)
```



	name
1344	Blackhole.D
30	Freezer.A
690	Freezer.A
866	Freezer.A
553	Freezer.A
1046	Blackhole.B
355	Blackhole.C

*Source: Webroot 2016, Verizon State of Security Report 2018, http://fortune.com/2017/09/14/google-play-android-malware/
RSA Conference 2018; Mac OSX Threats session By Trend Micro

AND MUCH MORE

- Social Engineering – Phone calls! Microsoft is never going to call you to tell you they found a problem/breach!
- Mobile devices are fair game!
- Apple Mac's are fair game too!
- Text/SMS messages
- Cryptojacking - Malicious mining via compromised websites
- Cryptomining - Malware-based attacks a user's device (CPU)
- IoT (Internet of Things) devices – Alexa, doorbells, camera's, TV's, Thermostats, and even your refrigerator. There is no anti-virus or firewall installed on these devices.

YOUR ROLE

What you can do to protect yourself, your family and your employer

OFFICIAL WORD ON PREVENTION…

63% of identity deception-based email attacks impersonate a trusted individual or brand.

Security awareness training for all employees can reduce your risk significantly.

- Make sure employees are aware of ransomware and of their critical roles in protecting the organization's data.
- Patch operating system, software, and firmware on digital devices (which may be made easier through a centralized patch management system).

*Source: https://www.fbi.gov/investigate/cyber 07-08-2018

IBT

I.T. SECURITY SUGGESTIONS

What YOU can do!

Passwords:

Strong passwords that rotate every 90 days

Example 1:

- Animal (static) Antelope
- 2nd Character cap aNtelope
- How many letters total? aNtelope8
- How many vowels? aNtelope84
- One character or symbol aNtelope84/

Example 2:

- Phrase: Crazy Hackers Can't Guess My Password
  1510 chcgmP1510*

IBT

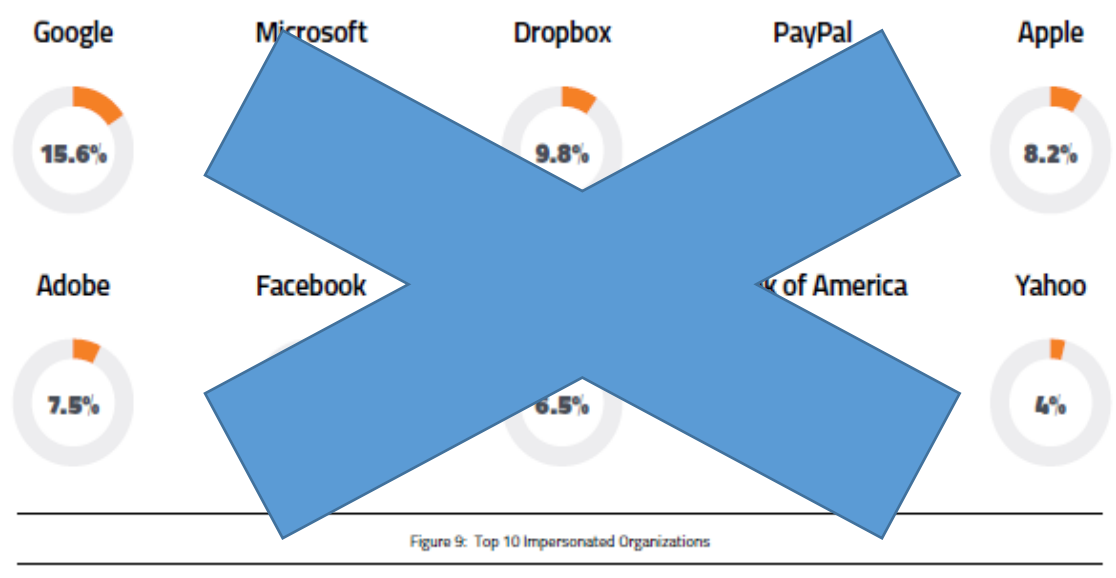
STRONGER IS BETTER

Number of Characters	Numbers Only	Lowercase Letters	Capital & Lowercase Letters	Numbers, Capital & Lowercase Letters	Numbers, Capital & Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15b years
16	2 days	34k years	2b years	37b years	1t years
17	4 weeks	800k years	100b years	2t years	93t years
18	9 months	23m years	6t years	100t years	7q years

Source: howsecureismypassword.net

IBT

RE-USE OF PASSWORDS



Use a password manager!

Examples: Keeper, Lastpass, 1Password

Source: Webroot 2019 Threat Report

I.T. SECURITY SUGGESTIONS

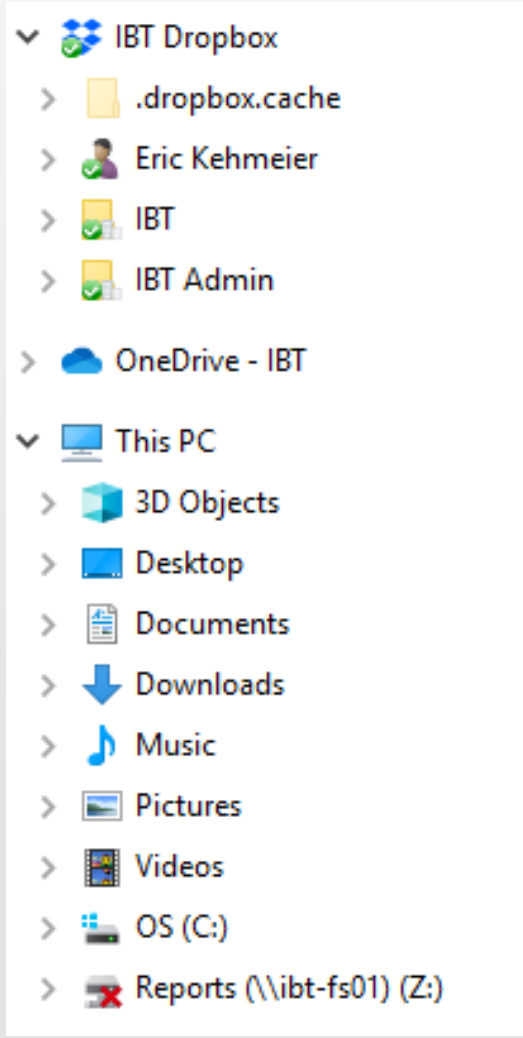
What YOU can do!

Data Saving:

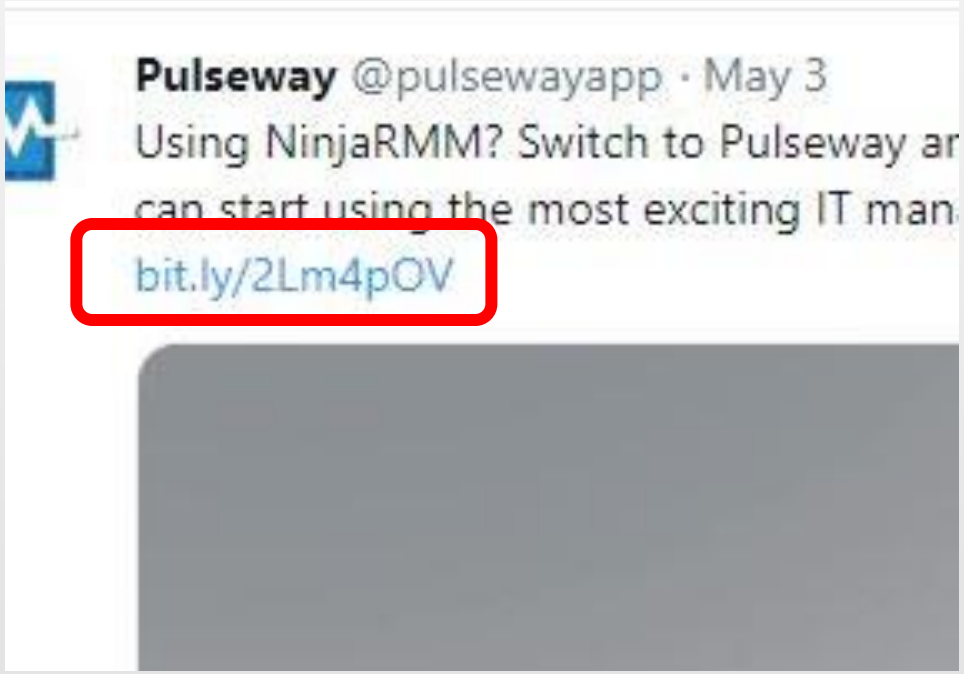
Must be on the (company name) server drives (not your desktop) or the company (One Drive, SharePoint, Drop Box, or other cloud-based storage).

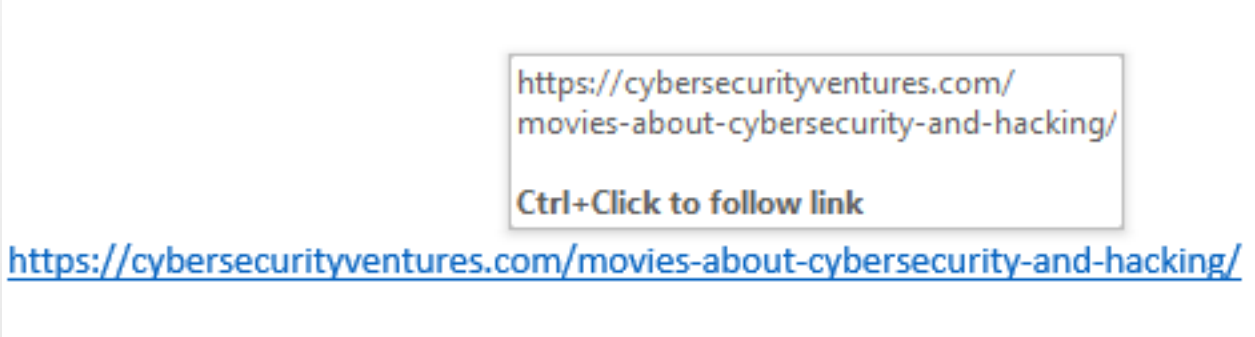
If accessing from home:

- ❑ Make sure your computer is updated with latest paid Anti-Virus, Anti- Malware updates /subscription
- ❑ Make sure your Windows Updates are turned on – spot check monthly.
- ❑ Restart your computer at least weekly to refresh and install pending updates.
- ❑ Follow remote worker policy



ABBREVIATED DOMAINS

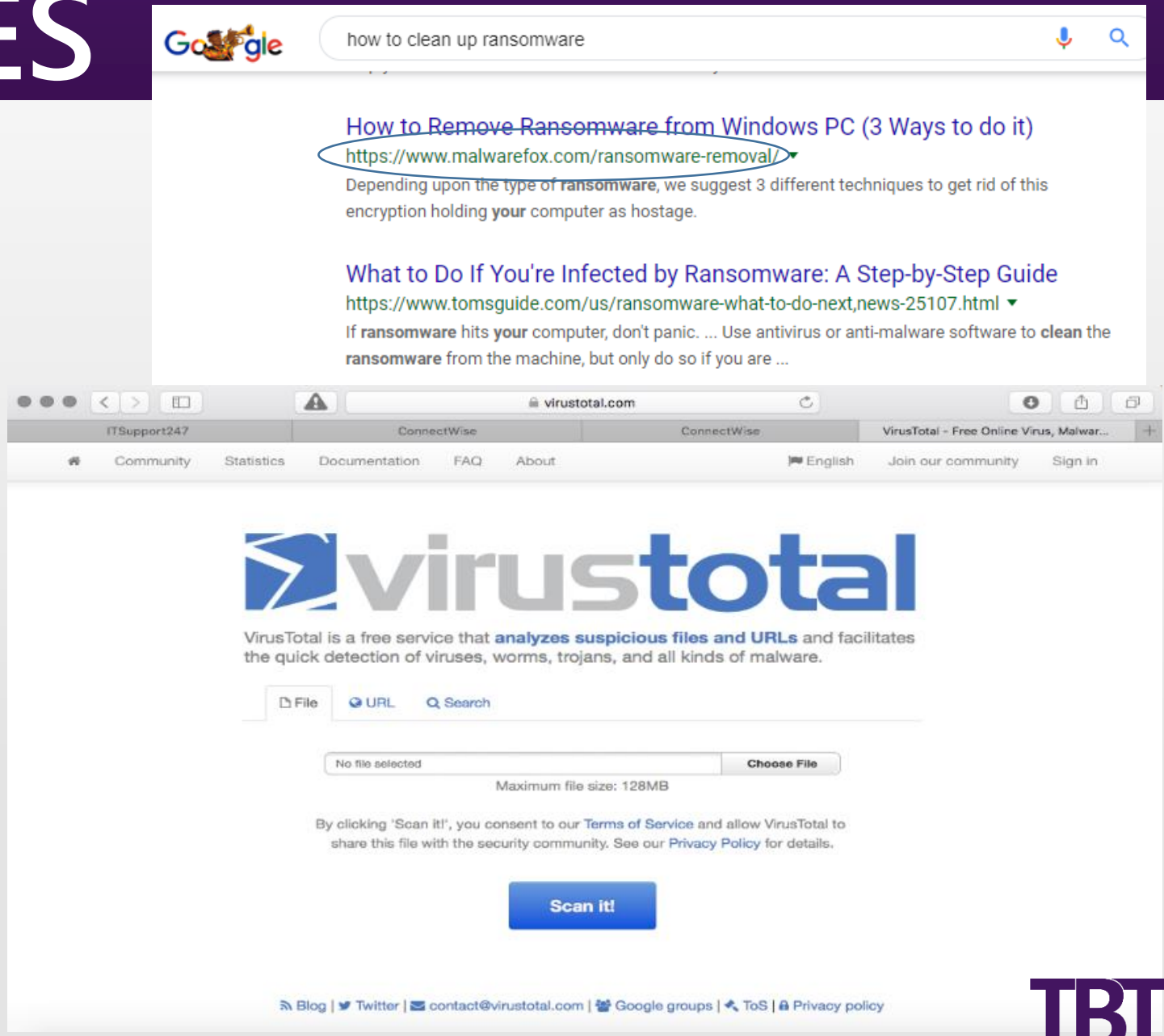




WEB SEARCHES

- Note the actual URL (green) that you are being sent to *Ignore Blue Header*

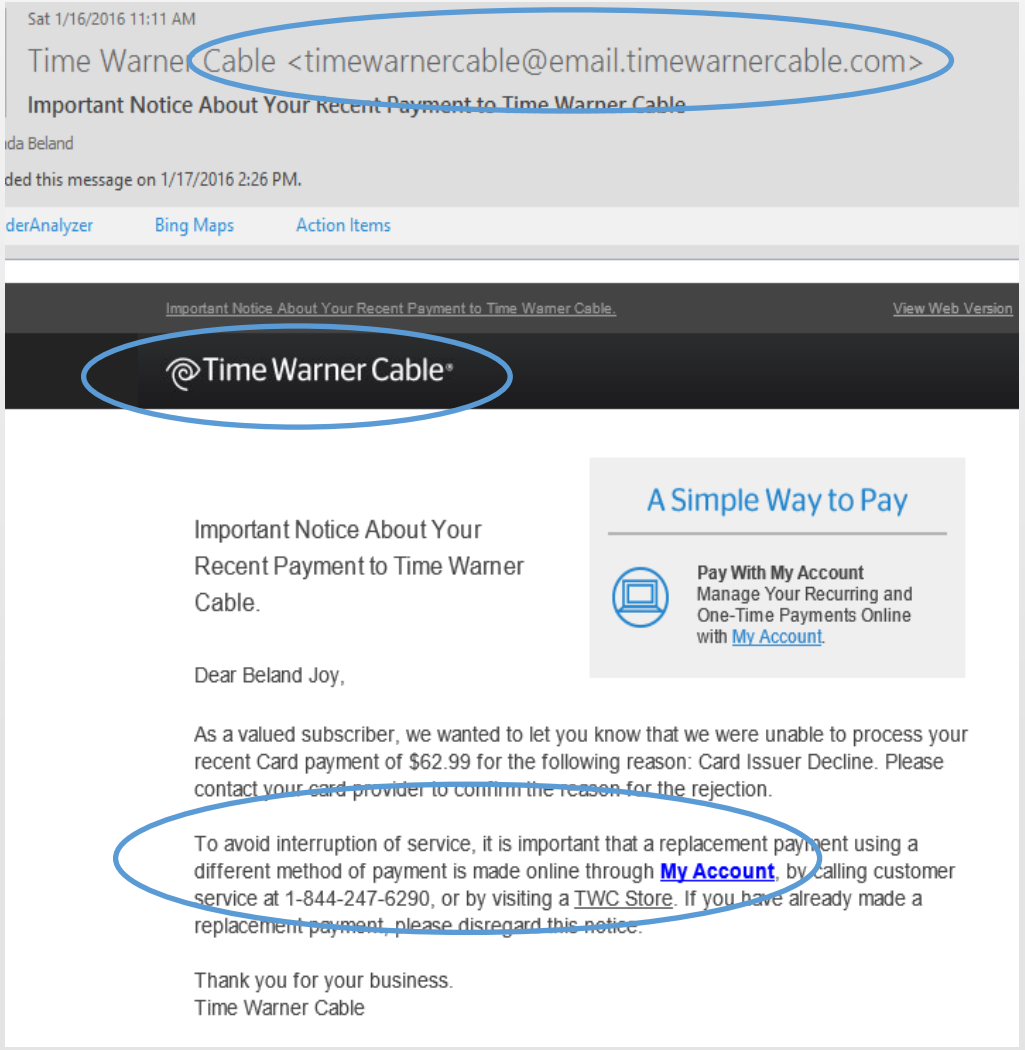
Unsure?
https://virustotal.com
to check it first



I.T. SECURITY SUGGESTIONS

What are the signs of a phishing email?

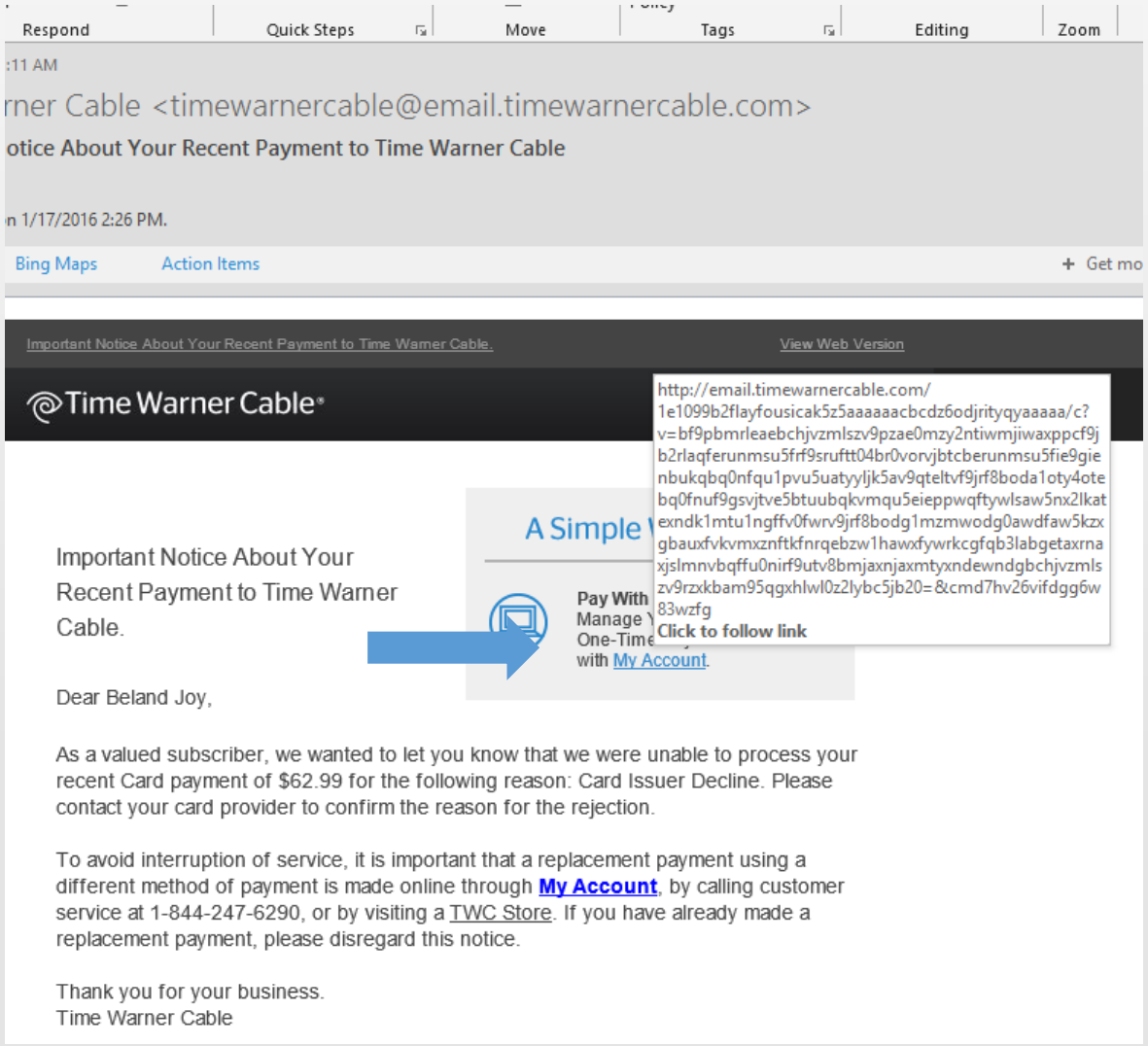
- Sender actual email address is not correct
- Logos misplaced, off color or missing all-together
- URL's to click on with an urgent request to take action immediately



I.T. SECURITY SUGGESTIONS

The URL “hover”:

- Be the master of your mouse.



HOW DO YOU THINK YOU'VE BEEN DOING SO FAR?

HOW DO YOU THINK YOU'VE BEEN DOING SO FAR?

1 of you clicked on the hyperlink in our test email. That's 9%. Way better than the average we see, which is upwards of 30% … but still, it's 9% more than we want!

Random Phishing Test Report - JAN 2019			
	IP	Event	Timestamp
@[redacted].com	162.208.94.226	open	2019-01-08T19:11:58.694Z
[redacted]com	162.208.94.226	open	2019-01-09T00:47:06.934Z
le@[redacted].com	99.112.138.7	open	2019-01-09T01:48:26.535Z
[redacted]com	167.89.85.54	delivered	2019-01-08T17:27:57.530Z
@[redacted]com	167.89.85.54	delivered	2019-01-08T18:40:40.057Z
[redacted].com	167.89.85.54	delivered	2019-01-08T18:44:10.080Z
[redacted]com	167.89.85.54	delivered	2019-01-08T19:31:15.670Z
ez@[redacted]com	167.89.85.54	delivered	2019-01-08T23:08:07.221Z
@[redacted].com	167.89.85.54	delivered	2019-01-08T23:11:56.570Z
[redacted].com	167.89.85.54	delivered	2019-01-09T00:54:25.895Z
@[redacted].com	162.208.94.226	click	2019-01-08T22:19:08.709Z

TIME TO SHIFT

WHAT you need to win

DOES THIS SOUND LIKE YOU OR SOMEONE YOU KNOW?

Do you cross your fingers and hope every time you hear about the latest cybersecurity breach, praying that you aren't using any of the software, scripts, or vendors impacted?

Do you have a wavering sense of security relying on the same cybersecurity protocols you've utilized for years, knowing deep down they're not enough to keep you safe?

Do you lay awake at night worrying what security threat is going to hit next and hoping that you'll have a clean enough back-up to be able to recover if you're impacted?

Do you think I'm not big enough, our data is sensitive, or it will never happen to us?

IBT

TIME TO SHIFT

There are 5 key shifts every business needs to make to ensure their business and employees are safe in a constantly-changing and more threatening world.

Once You Make Them...

You can focus on running your business

You'll have full confidence in your technology stack, whether your employees are working in the office or remote.

SHIFT #1

Acknowledge Your Weak Links.

- ❑ Employees are the primary cause of breaches
- ❑ Understand the full attack surface/what's at stake
- ❑ One simple mistake is all it takes to undermine years of hard work building up your organization's reputation
- ❑ Properly tune your tools, being only as efficient as the team or individual handling the tuning. More security tools are pointless if you aren't using the correct ones properly. (There is no silver bullet)

IBT

SHIFT #2

Support Your Employees Wherever they Are

- The lay of the land has changed in 2022. Workstations are no longer assumed to be confined within the locked office doors of a business outside of the normal 8AM – 5PM day.
- Thus – you need to keep in mind the following:
  - Have the right security tools
  - Tune these mechanisms effectively
  - Protect the full attack surface, wherever the employee may travel.

SHIFT #3

Compliance isn in Hand

- ❑ True or False – At ect your business's reputation
- ❑ True or False – Co turity insights
- ❑ True or False – Co ity-mindedness
- ❑ True or False – Wi liance businesses do not need to focus measures.
- ❑ Complacency wh edes every breach.

SHIFT #4

Ounce of Prevention is better than Pound of Cure

- Using a Hammer VS Using a Screwdriver
- In 2022, we speak with a ton of businesses who still think backups are a sufficient control to augment their security posture.
- This, contrary to popular belief, is a reactive use of the wrong tool for the job.
- Negotiating with Criminals VS Budgeting for Prevention
- Absorbing the cost of a breach is inherently more financially disruptive than paying for cyber security that prevents breaches.

CIO Magazine laid out good guidelines for IT budgeting and found that Small and Medium Business on average spent 6.9% of revenue on IT.

Source: https://www.techtarget.com/searchsecurity/tip/Cybersecurity-budget-breakdown-and-best-practices

IBT

SHIFT #5

Invest in Support

Accessibility & Security – A Fragile Balance

Accessibility is the process of creating products that are usable by people with the widest possible range of abilities, operating within the widest possible range of situations.

In IT Support, Engineers work to assist users to leverage technology to make their workday more efficient. When technology fails to meet its trusted expectation, that's where IT Support comes into play.

Where accessibility is added, security is always subtracted.

Security can be simply described as the quality or state of being secure.

In Cyber Security, SOC Engineers work alongside MSPs to implement various forms of security technology to prevent malicious activity entering a company's environment. In almost every form of security implementation, either cyber or physical, some form of Accessibility is sacrificed for higher levels of security.

Where security is added, accessibility is always subtracted.

IBT

WHAT YOU NEED TO WIN

1. Acknowledge Your Weak Links.
2. Support your employees wherever they are.
3. Compliance isn't security, but they go hand in hand.
4. Ounce of Prevention is better than Pound of Cure.
5. Invest in support.

These five shifts alone are enough to upgrade your cybersecurity posture and put you ahead of 88% of businesses.

And... You'll be able to sleep better at night!

IBT

RESOURCES

WHERE you can go to learn more?

INCIDENT RESPONSE

Signs of infection:

- ✓ Browser redirecting to a different website than what you'd expect
- ✓ Someone tells you they received an email from you that you did not send
- ✓ Popups that tell you your computer is infected or that you need to run a tool that you're not expecting and familiar with
- ✓ Computer slows down immediately after clicking something
- ✓ An overload of coupons or junk mail

- ❑ First step: Unplug the computer from the internet / network connection (demo blue cables on back of computers). If you're on Wi-Fi, turn off the Wi-Fi connection.
- ❑ Second step: Take a photo of the pop-up or website redirect with your smart phone and open a service ticket so we can receive the photo and advise on how to handle.

IBT

NOT JUST IN THE OFFICE, BUT AT HOME

583

TECH

Rarely Patched Software Bu Cripple Security

Wi-Fi devices, vulnerable to hackers, show difficulty o

By JENNIFER VALENTINO-DEVRIES

Jan. 18, 2016 11:58 a.m. ET

In late 2014, a small Massachusetts software company got an ominous email: A computer-security researcher said a flaw in one its programs put millions world-wide at risk of being hacked.

Engineers at the company, Allegro Software Development Corp., analyzed the flaw in the program, which can help users access the controls of home Internet routers. They quickly realized somethi strange: They had fixed this bug nearly 10 years...

Home routers are an easy target because mar largely on price, for devices that typically sell Customers acquire the routers either from re service providers. Once routers are sold, man incentive to update them to improve security use for years after what manufacturers term meaning they no longer issue updates.

The same problem is evident in smartphones for Internet-connected computers in everything from printers to television sets.

Of the endpoints reporting an infection, 68% were consumer devices, while 32% were business endpoints

Devices that use Windows 10 are at least twice as secure as those running Windows 7.

Source: Webroot 2019 Threat Report

IBT

I.T. SECURITY SUGGESTIONS

What you can do – iPhone Mobile Devices

- Turn on Apple iCloud/Find my iPhone, Review all settings
- Settings /Privacy
    - /Contacts, Camera
    - /Bluetooth Sharing
    - /Advertising
  - Settings /Privacy /Location Services /Look at list to see what is using your location
    - System Services /
      - Location-Based iAds
      - Frequent Locations
- Back up regularly using iTunes
- Don’t download any app that you don’t NEED if it’s not from an established company
- If you lose it, let your IT team know RIGHT AWAY

I.T. SECURITY SUGGESTIONS

What you can do – Android Mobile Devices

- All Mobile Devices should have a PIN (phones and tablets)
- Android devices should use Google Play Protect or Android Oreo for updates and security
- Use Brave Browser Ad Blocker (from Google Play Store)

Source: https://www.android.com/play-protect/
https://play.google.com/store/apps/details?id=com.brave.browser

IBT

CALL BLOCKING

FREE Apps from your cellular carrier!

- AT&T - Active Armor
- Verizon - Call Filter
- T-Mobile - Scam Shield
- U.S. Cellular - Call Guardian
- Sprint - Call Screener

Register you Cell Phone Number!

https://www.donotcall.gov/

Source: https://www.fcc.gov/call-blocking

IBT

CALL BLOCKING

Wireless Device Solutions

- Apple iPhones have an opt-in "Silence Unknown Callers" call-screening and blocking feature.
- Google Pixel phones have a "Call Screen" call-screening and blocking feature; Google offers several free, opt-in, call-blocking tool apps for Android phones; and Google Voice users can use a call management tool to block unwanted calls.
- Samsung partners with Hiya to offer a call-blocking solution called Smart Call to label potentially unwanted calls.

Source: https://www.fcc.gov/call-blocking

IBT

EXECUTIVES

The tip of the spear!

EXECUTIVE BEST PRACTICES

- Business
  - Remove your personal info from your website
  - Have a conversation with your Bank about security. They may have recommendations like Positive Pay for your business and could enable MFA on your accounts
  - Setup google alerts for your company and yourself
  - Is your employee handbook updated? This is where your computer and acceptable use policy is and that is what IT should be implementing
- Personal
  - Update your home router and computer (change wi-fi password yearly)
  - Lock your credit reports
  - Rotate your credit cards yearly (Read your statements)
  - Stop Junk Mail - www.optoutprescreen.com or call 1-888-567-8688

IBT

Five Things CEOs should Know

1. Cyber-attacks and security breaches will occur and will negatively impact your business. Today, the average cost of the impact of a cyber breach is $4.9 million.
2. According to most cybersecurity surveys, over 60% of all data breaches originate from unauthorized access from one of your current or former employees, or third-party suppliers.
3. Achieving information security compliance with one or more government regulatory standards for information security (i.e. ISO 27001, NIST 800-171, HIPAA, NYDFS, etc.) is good, but not sufficient to ensure real cybersecurity.
4. Cyber liability insurance premiums are significantly increasing in cost and often do not cover all of the damages caused by a cyber breach.
5. To achieve real information security and data resilience it is vital to combine managed Monitoring, Detection, and Response services with comprehensive disaster recovery and business continuity plans.

Source: https://www.bdo.com/insights/business-financial-advisory/cybersecurity/%E2%80%8Bwhat-ceos-should-know-do-about-cybersecurity

IBT

Ten Things CEOs should Do!

1. Ensure everyone in the organization from the top-down receives appropriate cybersecurity education and awareness training.
2. Hire an independent company to conduct a cyber risk assessment against government regulatory compliance requirements and industry standards to identify potential gaps in your company's information security policies, processes, plans, and procedures.
3. Verify that periodic penetration testing by certified Ethical Hackers is being conducted to identify potential cybersecurity vulnerabilities in your organization's information systems.
4. Require a timely and effective software patch management program be implemented by your Information Technology team to mitigate known security vulnerabilities as quickly as possible.
5. Ensure the organization has 24/7/365 monitoring, detection, and response capabilities for its information systems.

Source: https://www.bdo.com/insights/business-financial-advisory/cybersecurity/%E2%80%8Bwhat-ceos-should-know-do-about-cybersecurity

IBT

Ten Things CEOs should Do!

6. Verify the organization has an appropriate cyber breach incident response plan, including the policy and procedures related to ransomware attacks.
7. Hire an independent firm to conduct a cyber liability insurance coverage adequacy evaluation.
8. Establish information security key performance indicators (i.e. number of cyber-attacks, number of data breaches, network uptime, network downtime, cost of cyber breaches, cost of cyber insurance, cost of information security as a percentage of total company IT cost, etc.).
9. Ensure your company has well-documented and periodically tested disaster recovery and business continuity plans to quickly recover lost or stolen data to mitigate potential damages of cyber breaches.
10. Mandate additional layers of information security via encryption, multi-factor authentication, and highly restricted access to your company's most valuable information assets.

Source: https://www.bdo.com/insights/business-financial-advisory/cybersecurity/%E2%80%8Bwhat-ceos-should-know-do-about-cybersecurity

IBT

CYBERSECURITY CHECKLIST

For a copy of our 15-point checklist to protect your business from a Cyber Attack, please scan this QR Code.

IBT

THANK YOU!

Eric Kehmeier
ekehmeier@IBTsupport.com
www.IBTsupport.com
918.770.8738

Integrated Business Technologies
1800 South Elm Pl., Suite 200 / Broken Arrow, OK
918.770.8738 / www.IBTsupport.com