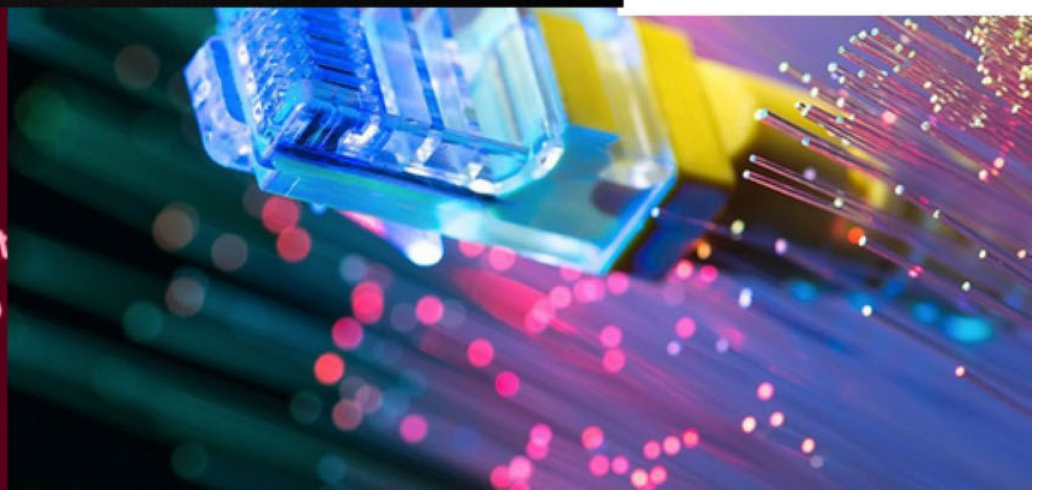
Cybersecurity Primer

ACCMA Briefing

1/27/2021

SHELBY COUNTY ALABAMA



CyberSecurity Training starts with the acknowledgement that **employees** are the weakest cybersecurity link.

Conversely, they're also the first line of defense against cyber attacks.

We need your help!

Some Stats - macro

- The global cost of cybercrime will reach <u>$10.5 trillion</u> by 2025

- Greatest transfer of wealth in history
- A business falls victim to a ransomware attack every 11 seconds..healthcare/govt

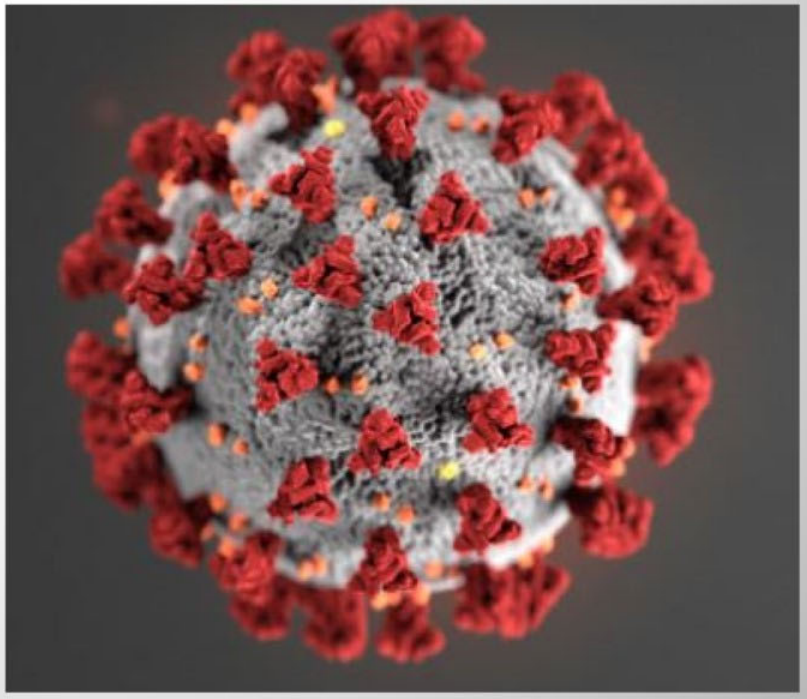
- More profitable than global trade of all illegal drugs combined.

If it were measured as a country, then cybercrime would be world's third-largest economy after the U.S. and China.

*Source: Cybersecurity Ventures 2021

COVID-19 is changing the world of work……

…..especially the cybersecurity threat landscape



Ominous Trifecta

Attack surfaces are widening

Threats are increasing

Budgets are changing

Attackers have the advantage more than ever.....

Industry analysis

"Vectors & Actors"

Incidents:	Total	Small	Large	Unknown
Total	32,002	407	8,666	22,929
Accommodation (72)	125	7	11	107
Administrative (56)	27	6	15	6
Agriculture (11)	31	1	3	27
Construction (23)	37	1	16	20
Education (61)	819	23	92	704
Entertainment (71)	194	7	3	184
Finance (52)	1,509	45	50	1,414
Healthcare (62)	798	58	71	669
Information (51)	5,471	64	51	5,356
Management (55)	28	0	26	2
Manufacturing (31–33)	922	12	469	441
Mining (21)	46	1	7	38
Other Services (81)	107	8	1	98
Professional (54)	7,463	23	73	7,367
Public (92)	6,843	41	6,030	772
Real Estate (53)	37	5	4	28
Retail (44–45)	287	12	45	230
Trade (42)	25	2	9	14
Transportation (48–49)	112	3	16	93
Utilities (22)	148	5	15	128
Unknown	6,973	83	1,659	5,231

- **21% Government Based**
- **77% involve employees**
- $1 cybercrime tools and kits
- 90% of cybercrime victims DO NOT report it
- Email responsible for spreading 92% of all malware
- U.S. target of 86% phishing attacks
- 70% of employees don't understand cybersecurity

2020 Data Breach Investigations Report

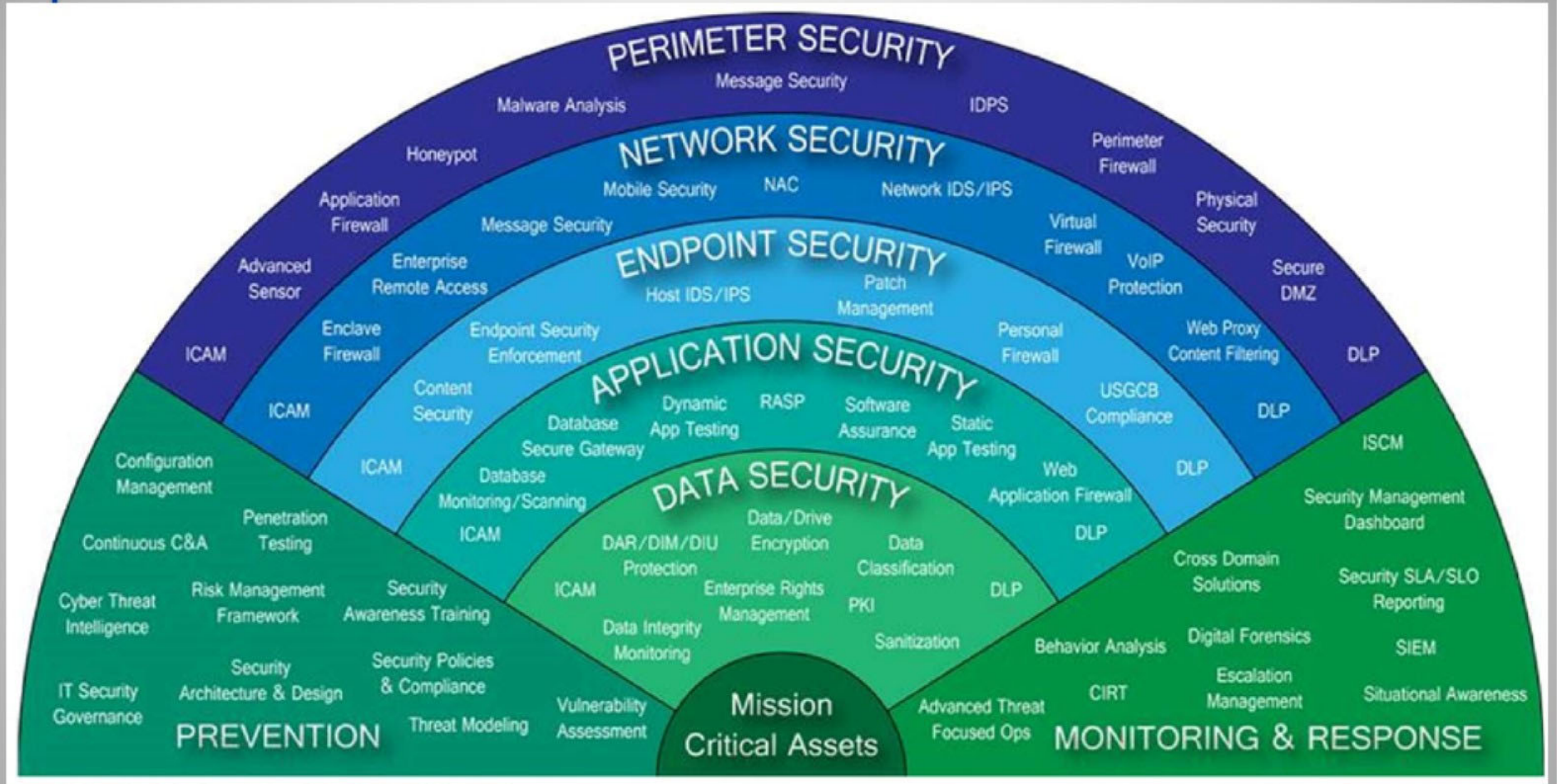
Source: 2020 Verizon Data Breach Investigations Report

2019-2020 Ransomware Attacks on Public Entities

More than 346 state and local governments broadsided by ransomware attacks

Source: The Ransomware War by PC Matic

Big Picture: CyberSecurity Encompasses hundreds of elements at different levels



Easy to get lost in the noise…..

Reality

- Changing tech behavior – culture item
- Focus on what will really mitigate risks
- **Education of employees is core**
- **<u>3 primary risks emerge</u>**

3 Major Risk Points

1. **Passwords**: The most critical aspect of password security is ***how*** employees use their passwords.
2. **Phishing**: The focus here is on identifying indicators of phishing emails. Ransomware payload
3. **Backups**: Now more important than ever…but are they current & tested?

1) Password Dilemma

- 98% of employees <u>do not</u> have a real strategy on passwords
- 60% of employees use the exact same password for everything they access
- 1961 technology….a problem

Creating Strong Passwords

- Develop a strategy. #s Only going up
- Use phrases or technology
- **Go Sea 5helby!** (easy to remember, spaces make it very secure)
- The phrase above is magnitude of orders more secure than "D@ught3rsN@m3!*%$#@!%-2020_1"

10 to 14 digits

LastPass

1Password
Put Passwords In Their Place

mSecure
Password Manager

Passwords

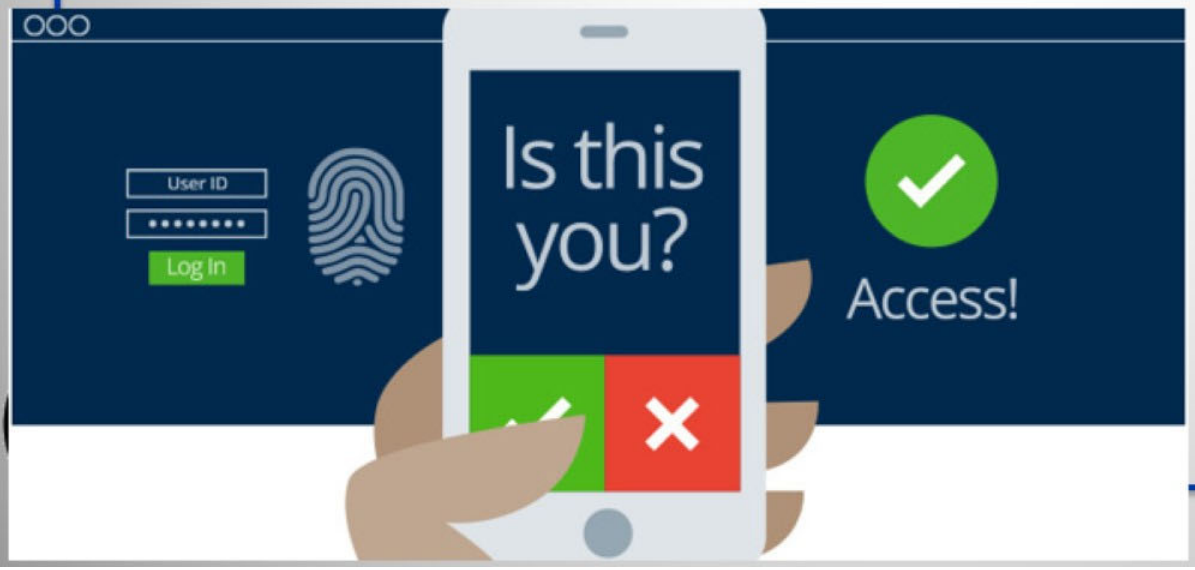
Password Length	Possible Combinations	Time To Crack (S = Seconds, M = Minutes, H = Hours, Y = Years)
4	45697	<1 S
5	11881376	<1 S
6	308915776	<1 S
7	8031810176	~4 S
8	208827064576	~1.5 M
9	5429503678976	~45 M
10	141167095653376	~19 H
11	3670344486987780	~.1 Y
12	95428956661682200	~1.5 Y
13	2481152873203 74E4	~39.3 Y
14	64509974703 2972E5	~1,022.8 Y
15	1677259342285 73E7	~26,592.8 Y
16	4360874289942 89E8	~691,412.1 Y
17	1133827315385 15E10	~17,976,714 Y
18	2947951020001 390E10	~467,394,568 Y

In 2010, an 8 character password would have taken 2.25 years to crack. The same password now would take under 2 mins to crack.

*Source: OSS.org

MFA (multi-factor authentication)

Best Practice on sensitive datasets



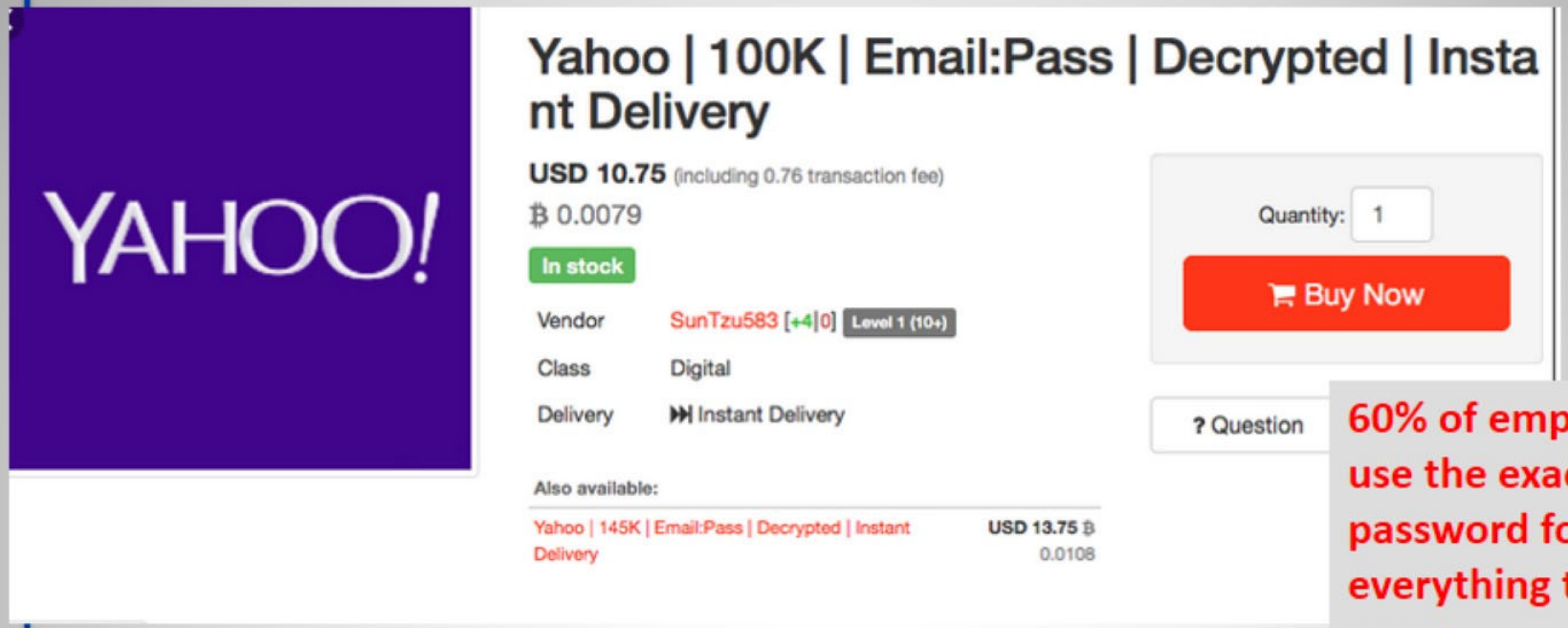
"2 Factor"

1) Something you know

2) Something you have

Password End Game?

Dark Web – Selling for less than $0.01 per email address & password:



60% of employees use the exact same password for everything they access

Surface Web

YAHOO!
Google
reddit
CNN.com
bing

4%

Deep Web

Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription only information
Some organization-specific repositories

96%
of content on the Web (estimated)

Dark Web

TOR
Political protest
Drug trafficking
and other illegal activities

Https://192.118.120.1

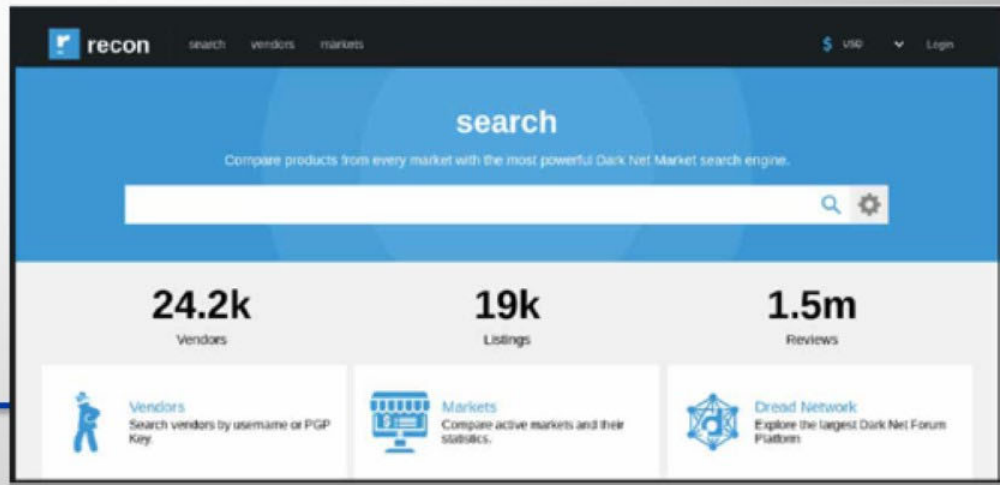
whonix
epic privacy browser
GLOBUS Free VPN Browser
Tails theamnesicincognitolivesyste
Tor

2020 Explosion in Dark Web Marketplaces

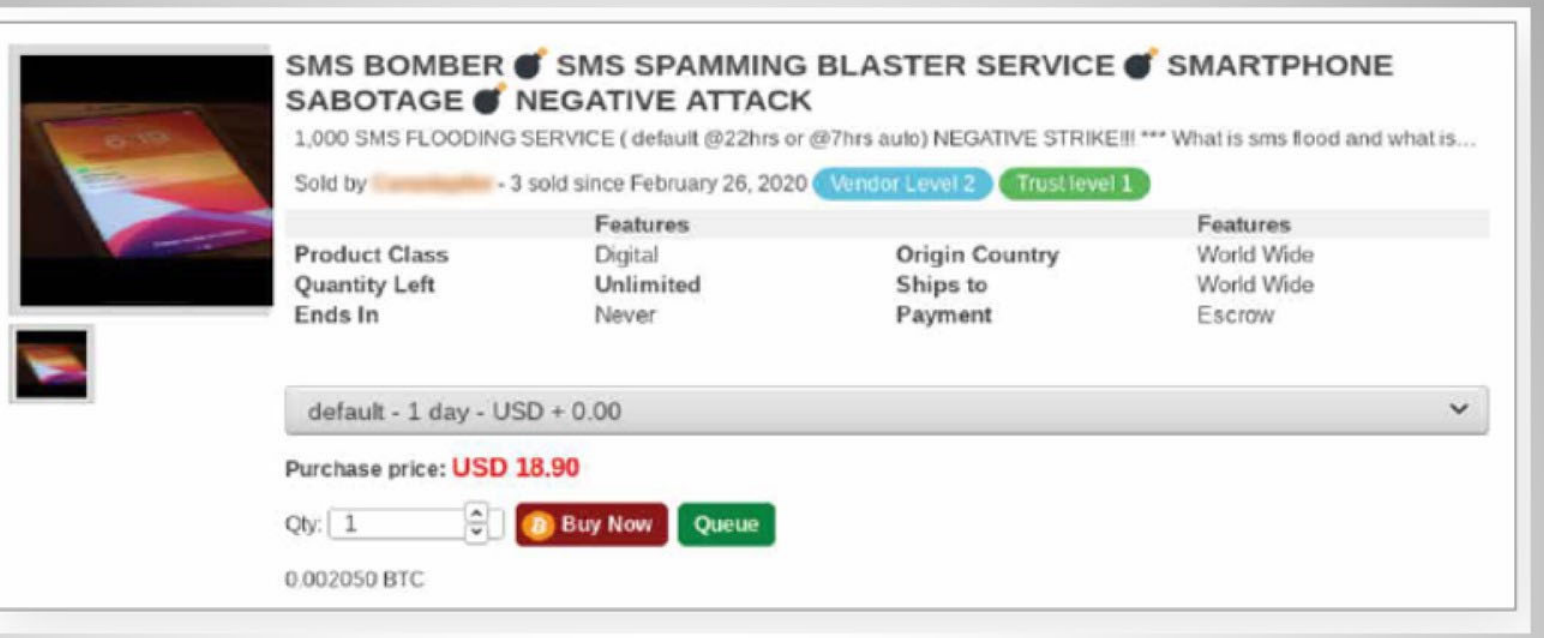
- Business Fullz
- Personal Fullz
- Ransomware Tools
- Remote Access Trojans (RATs), Exploit kits, Hacking Tools
- Remote Desktop Protocol Credentials
- Credit Card Credentials & cloned ATM Debit Cards
- Social Media Accounts
- Hacker University ----***degree costs $125***
- TV & Movie Streaming Accounts and Pizza Points
- Cryptocurrency

……and of course

- Drugs
- Human Trafficking



Dark Web Examples : CYBERCRIME-AS-A-SERVICE



SMS BOMBER 💣 SMS SPAMMING BLASTER SERVICE 💣 SMARTPHONE SABOTAGE 💣 NEGATIVE ATTACK

1,000 SMS FLOODING SERVICE (default @22hrs or @7hrs auto) NEGATIVE STRIKE!!! *** What is sms flood and what is...

Sold by [redacted] - 3 sold since February 26, 2020 Vendor Level 2 Trust level 1

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

default - 1 day - USD + 0.00

Purchase price: USD 18.90

Qty: 1 Buy Now Queue

0.002050 BTC

★*INSTANT DELIVERY* USA DOMINOS ACCOUNTS WITH 60+/120+ POINTS FOR A FREE PIZZA *ONLY 1.99$!*★

★*INSTANT DELIVERY* USA DOMINOS ACCOUNTS WITH 60+/120+ POINTS FOR A FREE PIZZA *ONLY 1.99$!*★ ✓F...

Sold by [redacted] - 576 sold since September 28, 2019 Vendor Level 6 Trust level 6

	Features		Features
Product Class	Digital	Origin Country	United States
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

60 to 120 points - 1 days - USD + 0.00 / item

Purchase price: USD 1.99

Qty: 1 Buy Now Buy Now Buy Now Queue

0.000216 BTC / 0.046193 LTC / 0.030925 XMR

Dark Web Market Rates – January 2021

CREDIT CARD WITH CVV NUMBERS

VISA/MASTERCARD					AMEX/DISCOVER				
US	UK	CANADA	AUSTRALIA	EU	US	UK	CANADA	AUSTRALIA	EU
$5-12	$15-20	$10-20	$5-25	$18-35	$5-12	$10-25	$15-25	$8-30	$18-35

TELEPHONE DENIAL OF SERVICE (TDOS) ATTACKS

NUMBER OF CALLS	TIME PERIOD	PRICE
3,000	48-hour period	$56.70
5,000	60-hour period	$94.50
7,000	72-hour period	$132.30
10,000	96-hour period	Contact seller for price

PAYPAL ACCOUNTS

AVG. PRICE	$50	$60	$80	$100	$200	$250-300	$500-550
BALANCE	$500	$600	$800	$1,000-2,000	$1,500-4,500	$2,500-8,500	$5,000-13,000

FULLZ DATA

ORIGIN	AVG. PRICE	ORIGIN	AVG. PRICE
US	$30-40	SWEDEN	$20-25
UK	$35-50	FRANCE	$20-25
CANADA	$30-45	GERMANY	$20-25
AUSTRALIA	$17-50	IRELAND	$20-25
ITALY	$20-25	MEXICO	$15-20

BUSINESS FULLZ DATA

Includes: Bank Acct Numbers, Employee Identification Number (EIN), Certificate of Business, Corporate Officers' Names, Birth Dates, SSN.)	$35-60

Dark Web: CYBERCRIME-AS-A-SERVICE

AVAILABLE CORONA VIRUS VACCINE $250

Vendor: [redacted] (99.5)

Dear Value Clients, IMPORTANT NOTICE>>>>>WE DO 100% REFUND or RE-SHIPMENT FOR ANY UNDELIVERED PACKAGE 'STEALTH' SHIPPING WORLDWIDE.

[redacted] offer the best AVAILABLE CORONA VIRUS VACCINE $250 at good and interested prices. ORDER NOW AND GET EXTRA BONUS ON REGULAR DEMANDS. OUR PRIORITY IS BASED ON MUTUAL TRUST. We offer Stealth and Discreet deliveries 100% guarantee, All our packages are at least double vacuum-sealed to ensure that our clients receive their package in perfect condition.
Contact me on wickr :[redacted]

WE OFFER OVERNIGHT DELIVERIES WITHIN THE USA AND EXPRESS DELIVERIES WORLDWIDE.

Our Costumers satisfaction is our Top Priority

Please when placing your order, make sure you provide us with the exact address where the delivery will be done.

For Fast and Easy Communication, Please kindly download the wickr me app from your App store or Google play and message us through our Wickr App Below.

Contact me on wickr :[redacted]

Price: Ƀ 0.012908 (250.00000000 USD)

S & H:

- USPS
  Ƀ 0.001033 (20.00000000 USD)
- UPS
  Ƀ 0.001033 (20.00000000 USD)
- OVERNIGHT DELIVERY
  Ƀ 0.001291 (25.00000000 USD)

Accepted Crypto Currencies:

Bitcoin

Ships From: United States

Ships To: Worldwide

BIY...

COVID-19 Antibody Test Kit

COVID-19 (SARS-CoV-2) Antibody Test Kit

Sold by [redacted] - 11 sold since March 26, 2020 Vendor Level 6 Trust level 6 4700 (5.00) 856 (5.00)

	Features		Features
Product Class	Physical Package	Origin Country	Europe
Quantity Left	73	Ships to	World Wide
Ends In	Never	Payment	Escrow

Registered Shipping - 10 days - USD + 11.25 / order

Purchase price: USD 44.98

Qty: 1 Buy Now Buy Now Buy Now Queue

0.004933 BTC / 1.071524 LTC / 0.702864 XMR

2) Phishing

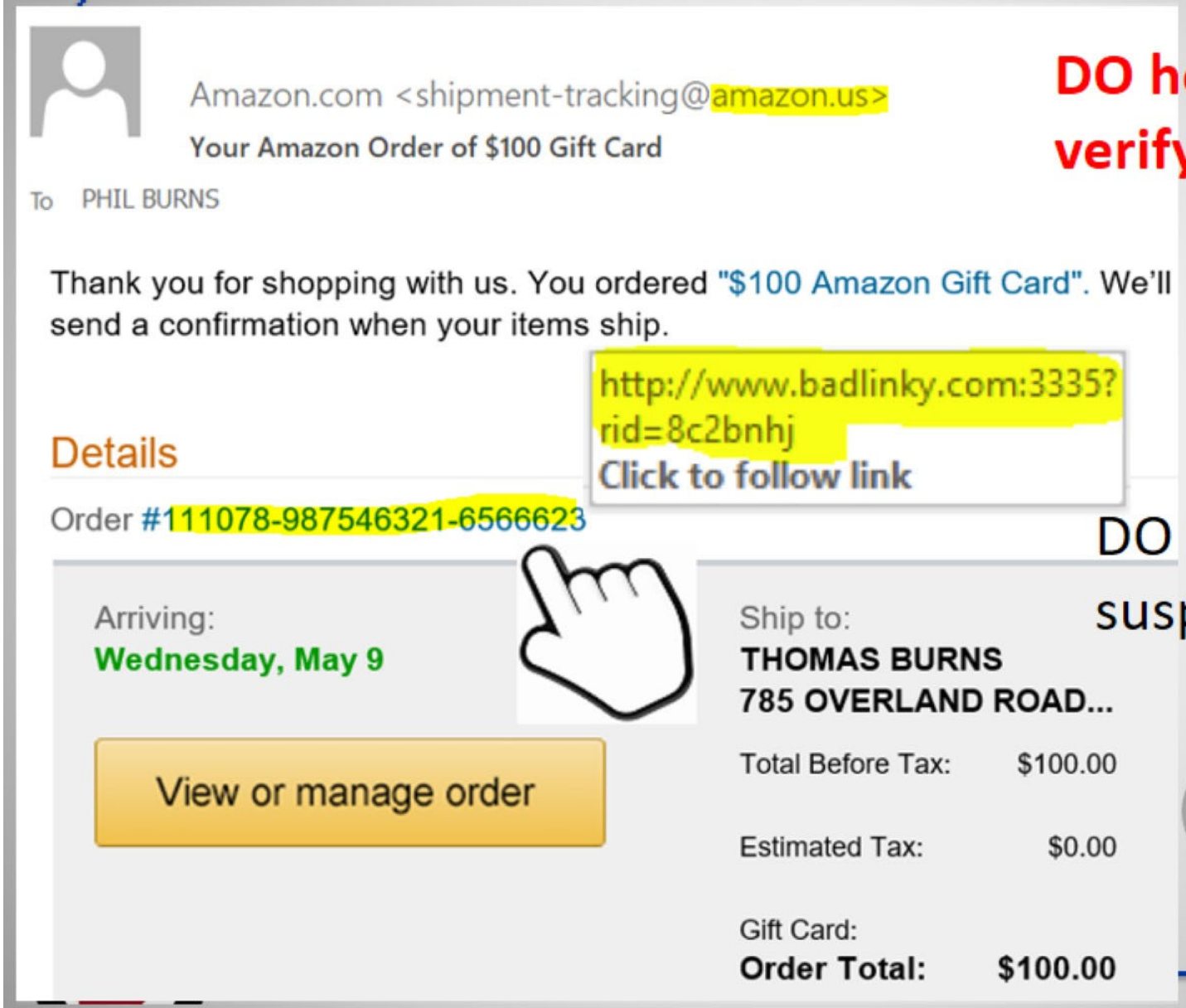
- Method of fraudulently acquiring sensitive information via trickery.
- Your employees are the primary targets, they need to be prepared, informed, weaponized as your first line of defense.
- <u>Training employees how to recognize and react to phishing (emails, txt or phone) is your best security ROI.</u>

Email

Text (Smishing)

Phone (Vishing)

Internal Phishing Campaigns



DO hover over links verify its location

DO NOT click on unknown links

DO NOT reply to suspicious requests

5% - 30

Gophish

3) Backups

- Backup has never been more important!
- No security measure is 100% reliable.
- Even the best hardware fails.
- Is your backup:

Recent?

Off-site & Secure?
Encrypted?
Tested?

IT "Device" Growth

Admin
Admin

Admin
1234

Admin
Password

Password
Password

Root
Admin

GOOD

CHEAP

FAST

	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2020
Root Admin	400	400	40	60	122	180	293	405	455	443	431	450	443
Password Password							683	856	911	968	1025	1050	1045
Password													
Admin Password			425	480	495	510							
Admin 1234							5098	7436	7685	8873.5	10062	11250	11168
Admin Admin	2180	2215	2346	2550	2680	2760							

8 Take Aways

- Use **extreme** caution when clicking any hyperlink within an email.
- Stay on latest version of operating systems (PC & Phone) and maintain all key security patches (to the extent possible).
- Only use business email for business. Many nefarious groups tap shopping sites email data.
- Only use business web browsing for business. Many shopping sites have a poor track record for controlling plugins and other code running on their sites.
- Do not use online email at work (while on a networked device). Many security layers are bypassed by opening external mail on network.
- Encrypt mission critical data stores on PC's, Servers and ALL portable data which includes iphones, USB thumb drives, tablets, laptops, etc.
- Ensure core Servers & PC's are backed up on a regular schedule
- Ensure virus/malware control are up to date and active on all PC's that are used – home & work – any data at rest (thumbs, cloud storage, etc.)

SHELBY COUNTY ALABAMA

veeAM

Gophish

1Password
Put Passwords In Their Place

TREND MICRO

LastPass •••

mSecure
Password Manager

https://haveibeenpwned.com/