

## ***Fraud Schemes Targeting Seniors***

---

*November 30, 2023*

**M&T** Bank

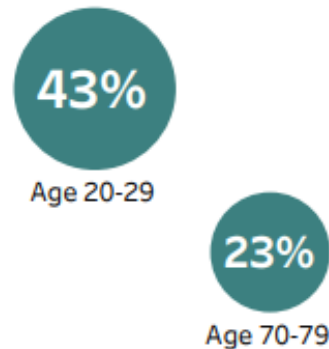
## A Wealthy Generation

- BABY BOOMERS represent the largest and wealthiest generation in U.S. history
- ELDER Financial Exploitation is the most common and fastest growing form of seniors and vulnerable adults
- AARP reported \$28.3 billion was stolen from older Americans in 2022
- 72% is stolen by a friend, family member, caregiver or someone known by the victim

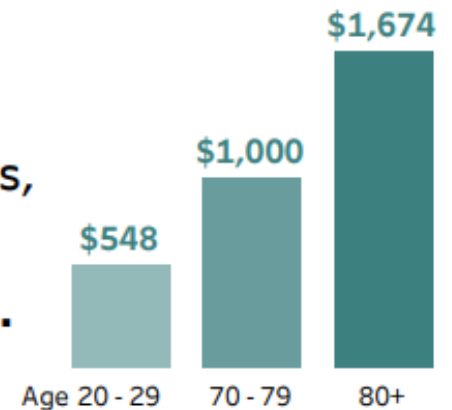


# Fraudsters Steal More From Older Americans

**Younger people** reported losing money to fraud **more often than older people.**



**But when people** aged 70+ had a loss, **the median loss** was much higher.



Source: Consumer Financial Protection Bureau

# Why are the elderly vulnerable?



- Lonely
  - Many living alone and grieving the loss of a spouse
  - Without close friends and relatives checking in, it's easy for strangers to step in and befriend for financial gain
- Memory Loss
  - 1 in 10 people 65+ has Alzheimer's / dementia
  - 7.2 million Americans are living with Alzheimer's / dementia
- Silent
  - Proud generation – elder abuse is vastly under-reported

## Government Imposter Scams

- Fraudsters pretend to be from the IRS, Social Security and other gov't agencies
- Claim you owe more taxes OR they can help you increase your benefits OR there is a warrant out for you
- Calls can appear to be coming from a gov't agency but are actually coming from fraudster overseas

Government agencies almost always communicate by letter delivered by USPS



# IRS Impersonation Scam

## ■ Scammer Tactics

- Search obituaries looking for widow/widowers — obituaries reveal great deal of information on potential targets
- Mailing letters or referencing collection notices sent via mail
  - *“We sent several notices in the mail which you failed to respond. Since you didn’t respond we had to call you directly”*
- Urgency! *“Payment must be paid now to avoid embarrassment of jail time”*  
Caller will stay on phone until payments are made
- Discourage victim from telling anyone
  - *“Don’t go to the local police because they will see an arrest warrant in the system and sometimes it can take months to clear”*
- Once successful, the victim will be targeted again
  - Scammer will call back for additional tax payments or targeted with a new scheme

# New Social Security Scam Letter



## Social Security Administration

Date: January 6, 2024

Case ID: SSA9903-330U

**SUBJECT: Suspension of SSN due to Criminal Activities**

Attention,

Due to fraudulent activities, your Social Security Number (SSN) will be suspended within the next 24 hours.

We are writing to inform you that your Social Security Number is being suspended due to the FTC's discovery of unlawful activities in Texas involving your identity.

Your case has been referred to the Department of Justice for prosecution under the Criminal Code Act 1950 and other Texas criminal offenses, including the Proceeds of Crime Act 2002 for:

1. Count 1 (Drug Trafficking) Act 258 Section D
2. Count 2 (Money Laundering) \*\*\* Act of 1986
3. Count 3 (Theft by Deception) Texas Supreme Court Code conduct 1986

A legal complaint has been filed against you as of today. In accordance with our standard operating procedures, law enforcement agencies have uncovered 25 bank accounts opened with your Social Security Number to perpetrate a \$14 million fraud. In the entire state of New Mexico, these accounts were used for unlawful activities such as money laundering, narcotics trafficking, and Internal Revenue Service (IRS) fraud.

The department attempted to deliver legal documents to your most recent known address, but US Marshals who made a visit discovered the house deserted.

If you have received this email, it implies that we have exhausted all other means of contacting you; if you are innocent of the allegations, please contact the OIG at the number shown below.

To plead yourself, you can contact the Office of Inspector General (Social Security Administration) at +1-800-465-1741.

A handwritten signature in black ink that reads 'Ken Paxton'.





# Lottery Scams



- Bad guys use real and fake lottery names: “Publisher’s Clearing House,” “National Sweepstakes,” “Powerball,” “Mega Millions” and others
- They claim you won but you need to pay the taxes up front
- Legitimate lotteries take taxes out of winnings
- You can’t win a lottery unless you are a citizen of the country of the lottery



# Grandparents Scam

*You: Hello*

*Caller: Hi Grandma!*

*You: Is this Emily?*

*Caller: Yes, and Grandma, I need your help!*

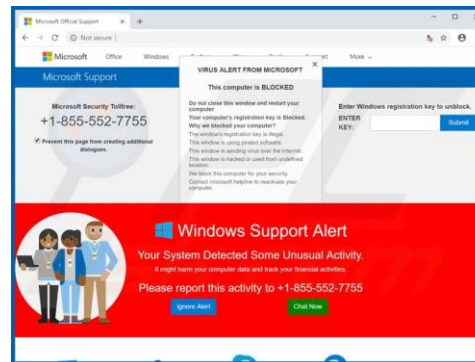
Scammers can easily get information on you and your loved ones from newspapers, Facebook and other social media sites

## *Avoid the Scam*

- *Don't react too quickly. Act with your head, not your heart*
- *Ask a question only the loved one would know*
- *Call Emily or another family member*






# Computer Virus Scam



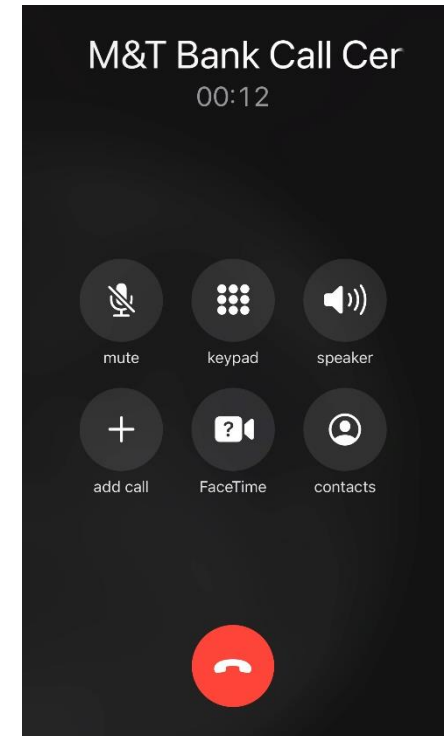
- Scammers are trying to get you to pay them to “fix a nonexistent problem with your computer or device.
- Allowing them in could result in installation of malware that can steal your info or damage your data or device
- If you get a phone call, hang up. If you get a text, delete it
- If you get the pop up, log off your computer
- Source: Microsoft: Protect yourself from tech support scams. Support.Microsoft.com/security

## Impersonation: Real Life Scenario

<b>Situation</b> 	Receives wire instructions via email and confirms by calling Title Company. Customer comes into branch and processes wire. Wire instructions had changed via email. ( <i>customer admitted this during investigation</i> )
<b>Attack</b> 	Fraudster was reading emails between our customer and Title Company and changed payment instructions last minute.  Funds were moved quickly
<b>Impact</b> 	<b>Six-figure loss</b> to customer

# Phone Number Spoofing

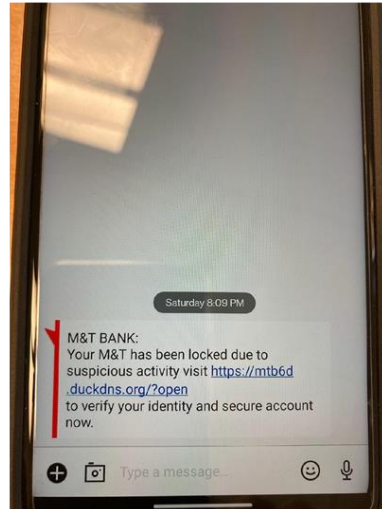
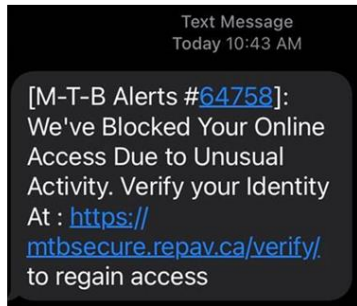
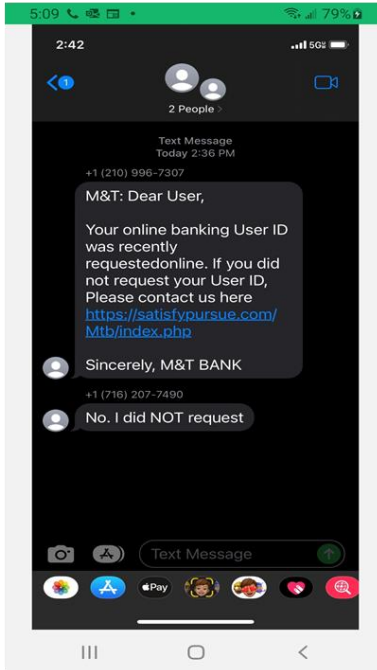
- Fraudsters continue to call customers from legitimate bank 1-800 numbers including M&T
- Customers reveal account numbers, PII and passcodes



# Fraud Department Scam

- Starts with a text message from Bank Fraud Department:
  - Fraudster: Did you authorize a \$589 purchase to xxx company?
  - Customer: “yes”
- Incoming call from ‘Bank.’
  - Fraudster: “Good afternoon, am I speaking to ‘customer name?’ “Did you recently sign into your Chase account from Omaha using a Samsung Galaxy phone?”
  - Customer: No! I’m in Buffalo, NY
- Fraudster: “No worries, I’ll help get this straightened out. It looks like someone has hacked into your account. You won’t incur any charges but it looks like I’ll need to verify some things with you.”
- In the next five minutes, they gain trust, log in to customer’s account and send a one-time passcode to customer’s legitimate phone. Customer gives passcode to fraudster
- Within minutes, account is drained with Venmo and Zelle payments

# Smishing



Text Message  
Today 9:01 AM

[alerts@M&T/BANK]: Your transfer of \$198 to acct ending \*\*7628 was successful. If you did not do this please cancel/report fraud mtbsecure.ga/report

Text Message  
Today 9:37 AM

M&T: Did You Attempt A Zelle Payment Of \$950.00 From Your Account? Kindly Verify here <https://arronkinggenesh.com/mtb/index.php> If you did not Request this.  
Sincerely,  
M&T BANK

Text Message  
Today 12:13

M&T Bank: The Zelle(R) payment sent to LISA REYES is under review. If you did not initiate, visit <https://kav6.io/0/3STgAU> to regain access. D

Wednesday, April 6

M&T ALERT : Your Online Account Has Been Revoked Due To Suspicious Activities To Restore Visit: <https://www.ajwebtechnologies.com/M&T/>

11:54 AM

Text Message  
Today 1:12 PM

M&T: Your one-time verification code is 571-305. If this is not you Kindly Follow: <https://st-art.us/m-t-b.php?page>



# Mail is in Jeopardy – this means checks!

NBC NEWS

Postal worker among 3 charged in \$24 million stolen check scheme, officials say

SHARE & SAVE



## Postal worker among 3 charged in \$24 million stolen check scheme, officials say

The checks were stolen from the mail and offered for sale through a Telegram channel, federal prosecutors said.



<https://www.axios.com> › Technology

### Trending crimes: "Check washing" and "mailbox fishing"

Nov 16, 2022 — Trending crimes: "Check washing" and "mailbox fishing" · Criminals are branching into **stolen** account numbers and identity **theft**, and selling the ...

LACKAWANNA COUNTY

## Break-ins reported at USPS mail collection boxes

The postal inspector says it was most likely thieves trying to steal people's checks.



## Hamburg Police provide advice in wake of mail thefts

Town of Hamburg Police are investigating thefts from 3 or 4 mailboxes. Thieves are then altering checks to steal money from people.



abc11.com

<https://abc11.com/mail-theft-postal-carriers-check-w...>

### Thieves target postal carriers, mail drop-offs in attempt to steal ...

Dec 15, 2022 — Maimon said thieves are getting the stolen checks by either swiping ... in mail theft incidents -- such as **mailbox thefts** and postal carrier ...





## Find 8 details that can be used to commit fraud

Michelle Cents  
123 Penny Drive  
Dollarsville, US 12345

5719

DATE: May 1, 2020

PAY TO THE ORDER OF: ABC Water Company \$ 110.52

one hundred ten and 52/100 ----- DOLLARS

MEMO: April Water Bill Michelle Cents

⑆000045678000 0000⑆ ⑆0000

 Security Features Detailed on Back.

## Find 8 details that can be used to commit fraud

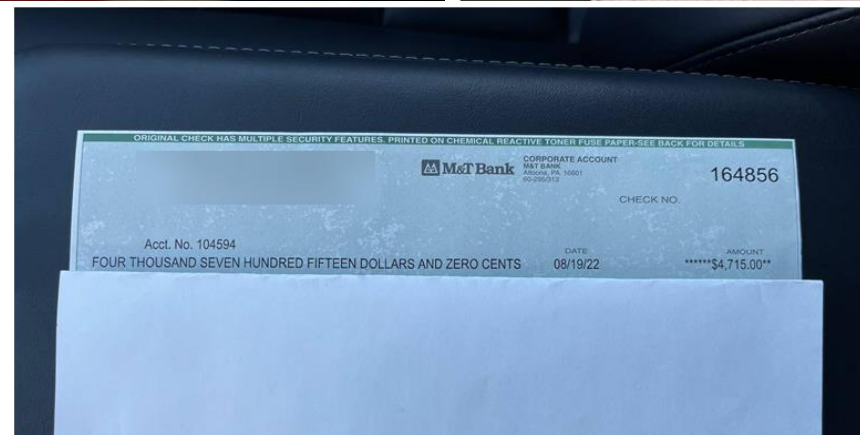
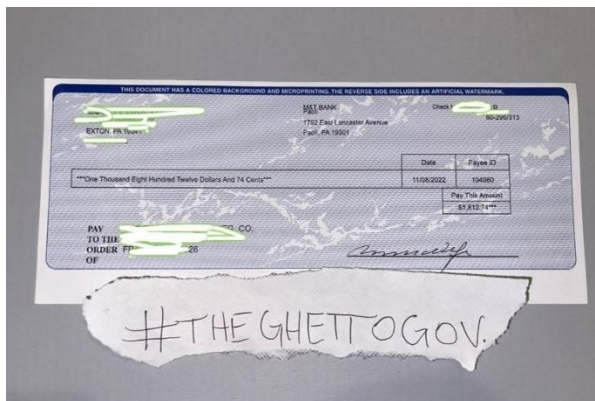
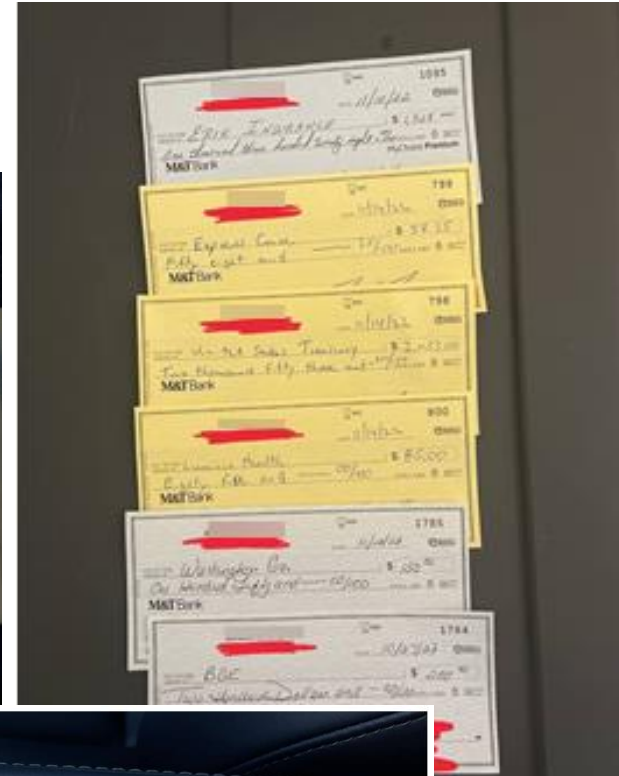
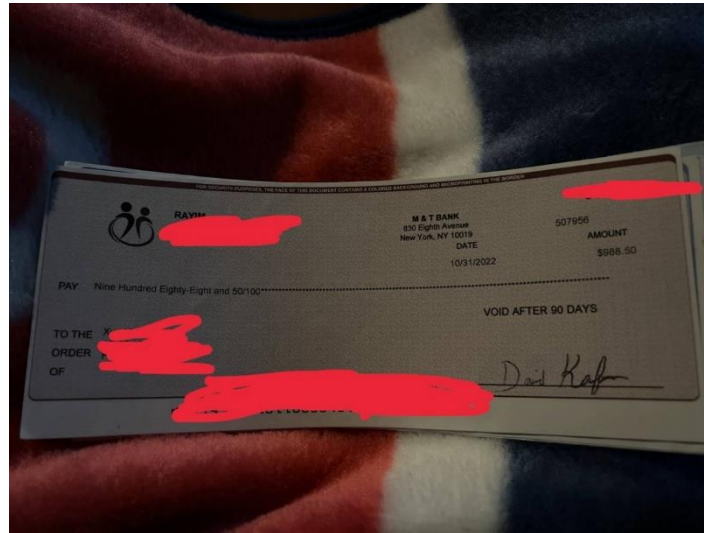


1. Maker info – applied to counterfeiting checks
2. Bank name – can lead to account takeover
3. Check number – gives a fraudster the range when counterfeiting
4. Maker signature – for replication
5. Routing and account number – aids with ACH fraud
6. Check stock – layout to be replicated
7. Memo line – adds legitimacy when counterfeiting
8. Payee Line – Forged endorsement risk; synthetic fraud



## Checks for Sale

- Telegram as well as other social media sites have vibrant marketplaces for buying and selling customer information, account and card details.



# Phishing Attacks

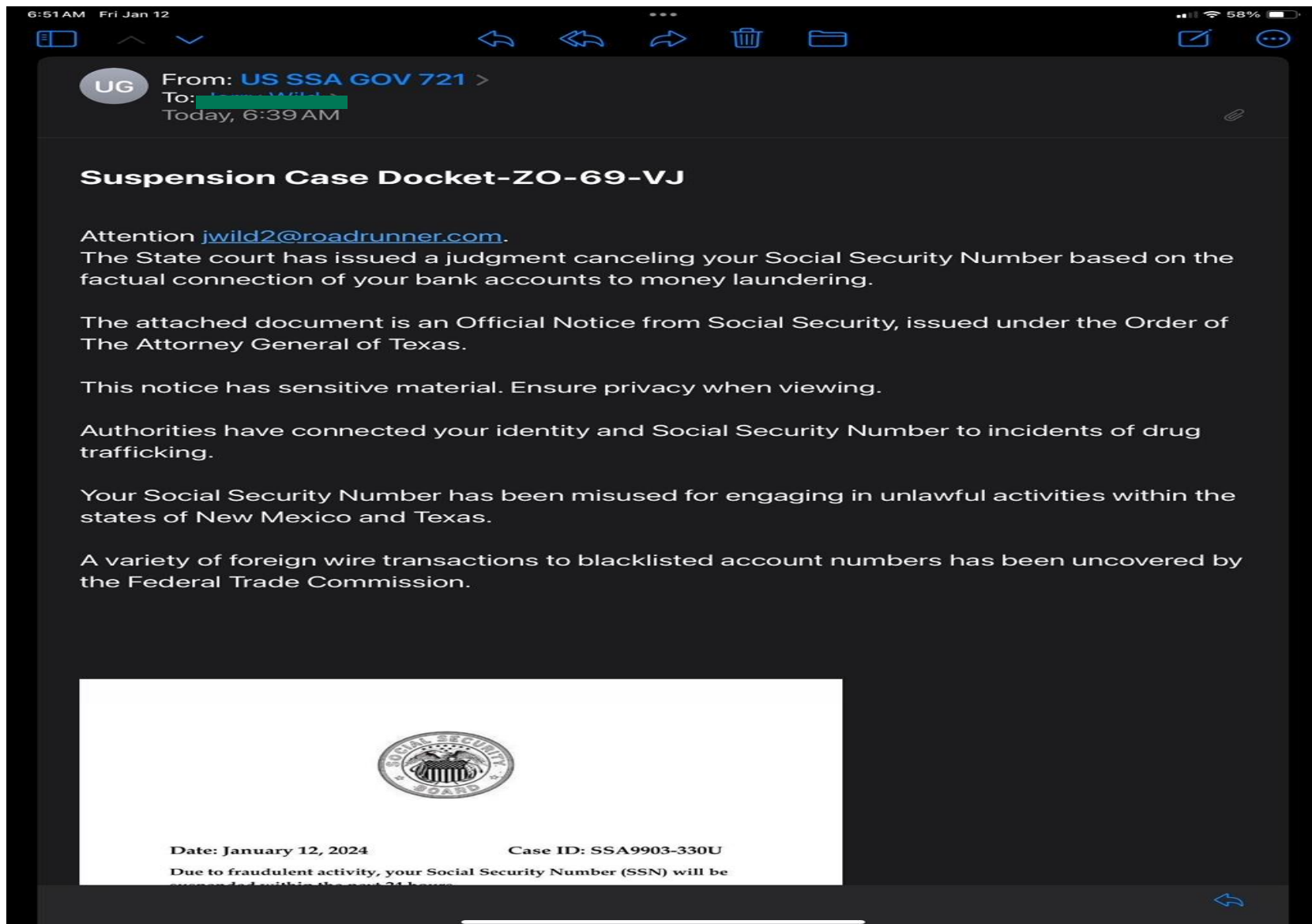
**91%** of cyber attacks started as a phishing email



Phishing attacks **PREY** on curiosity, greed, great deals and emotion

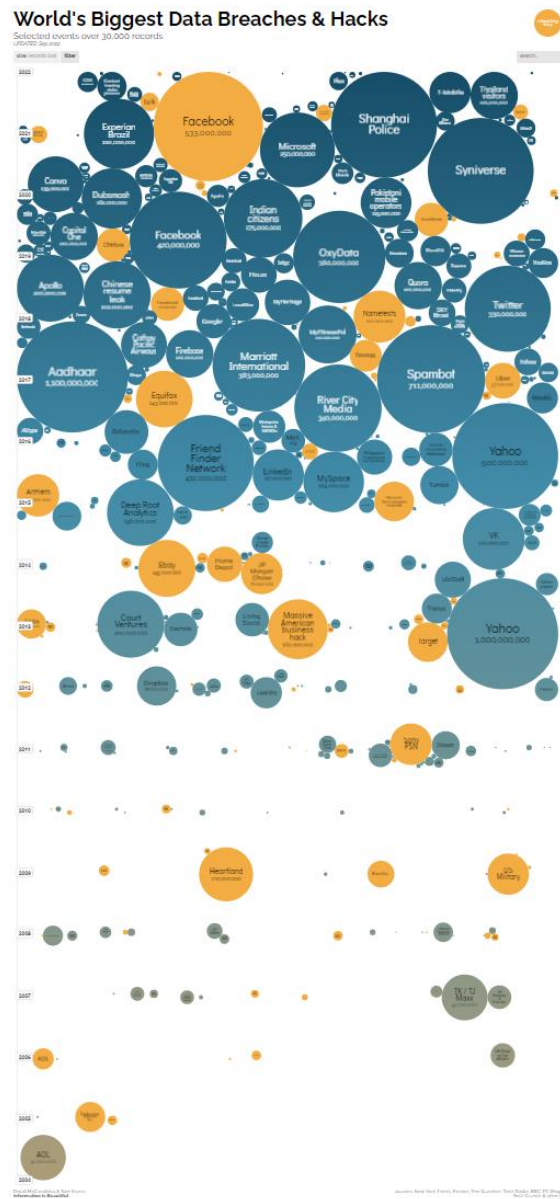


A successful phishing attempt could **STEAL** your credentials, passcodes and place malware on your computer



Email that sent is  
workneshokadigbo77@gmail.com

# Breaches





# World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

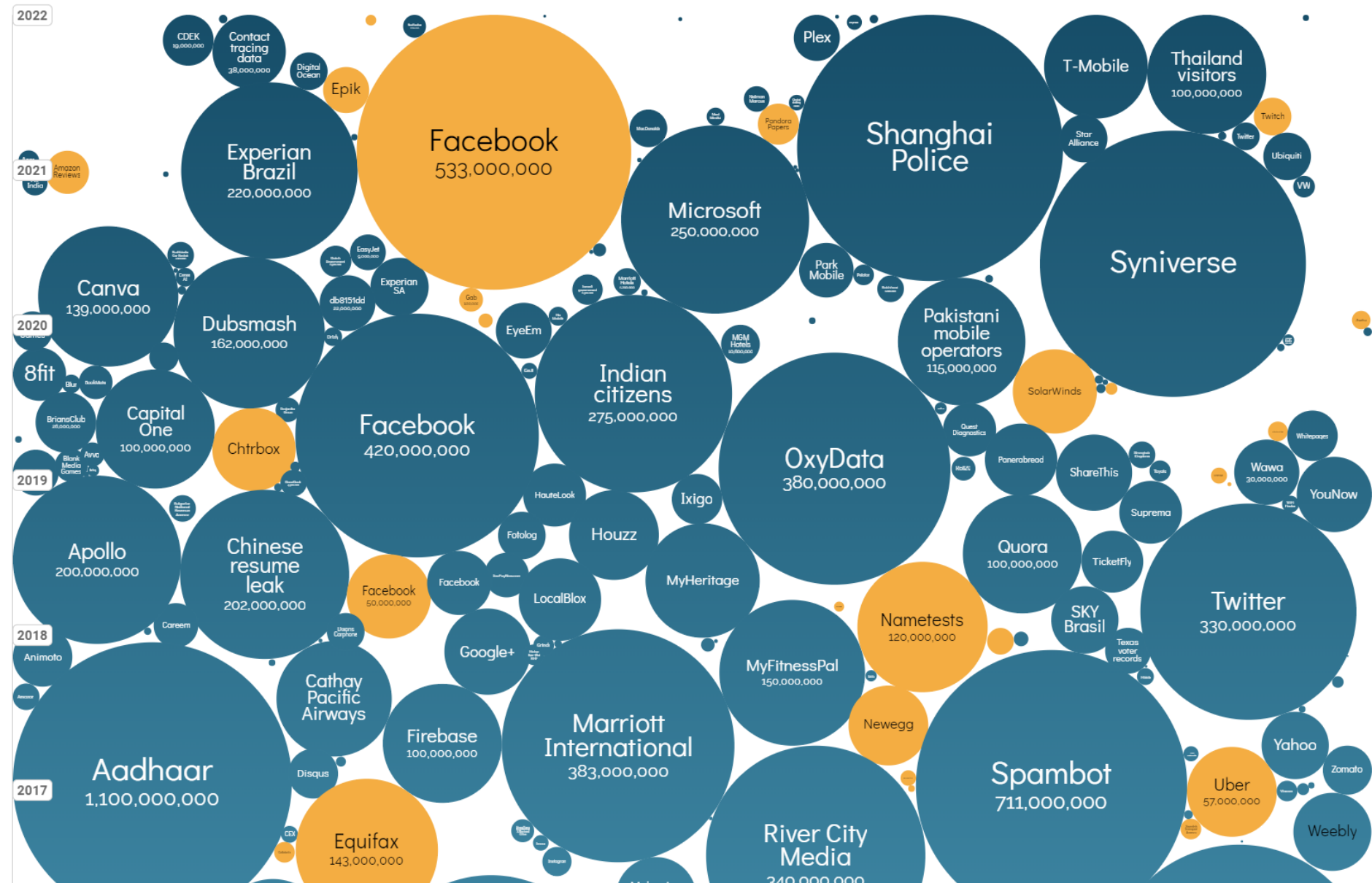
UPDATED: Sep 2022

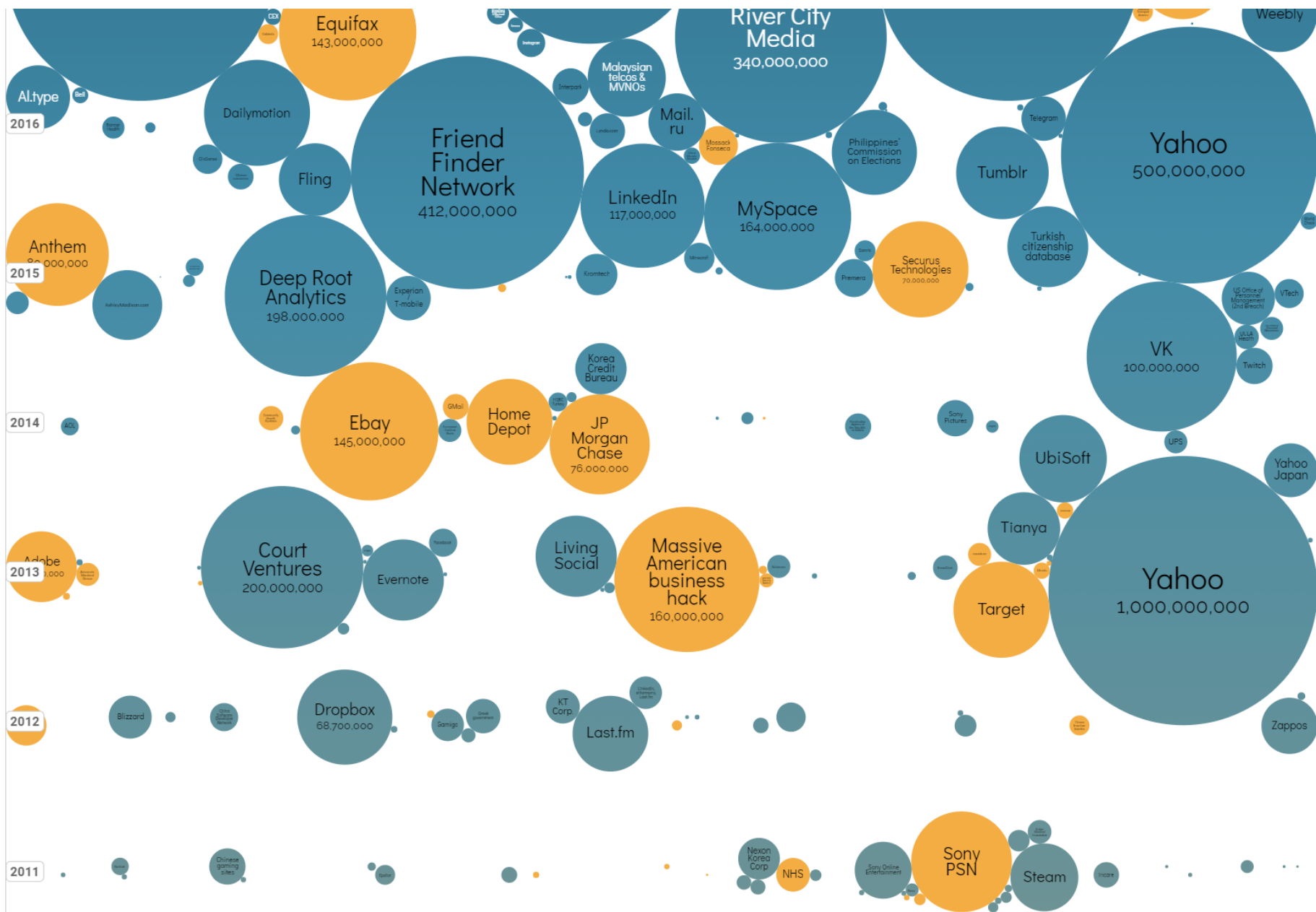
interesting  
story

size: records lost

filter

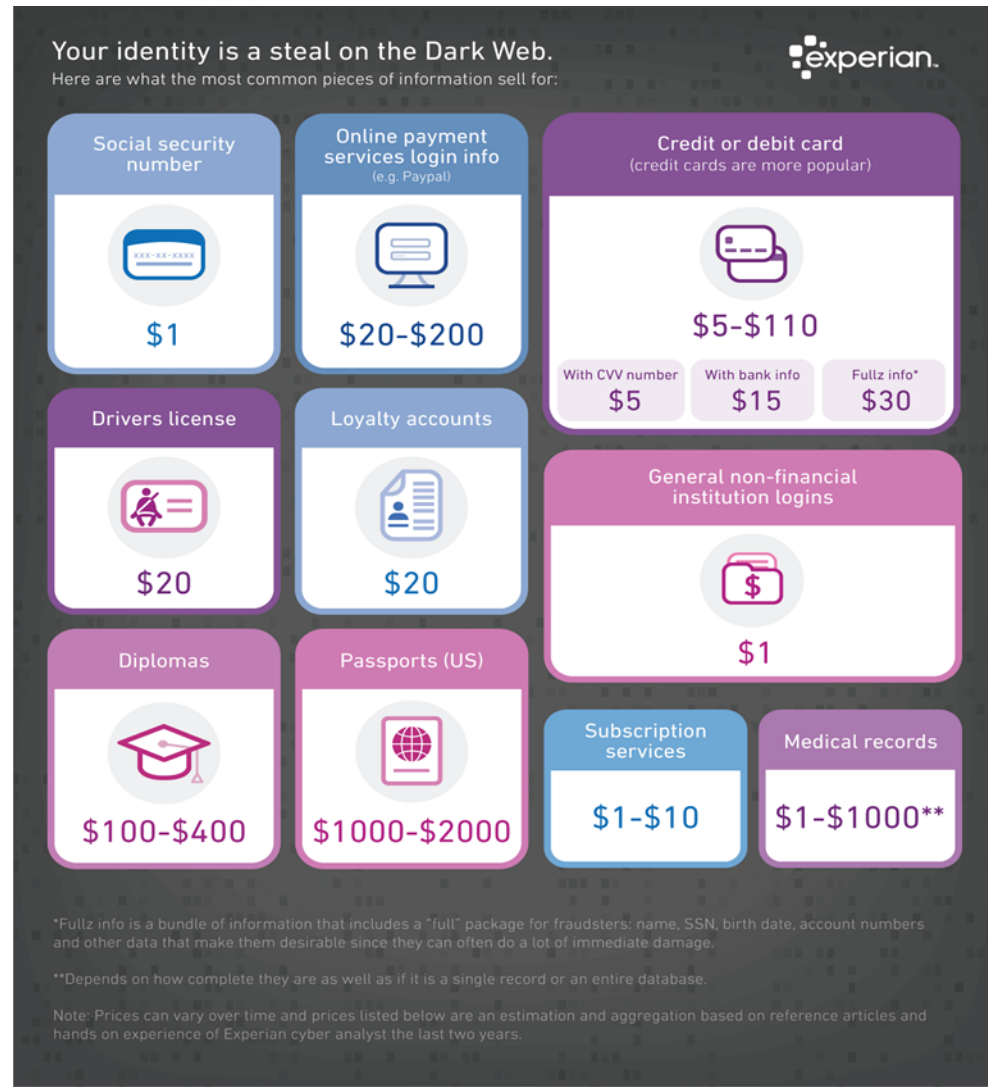
search...





## What is your data worth?

- Prices based on supply and demand
  - Drivers License \$20
  - Lowest cost items are SSN as they are widely compromised
- Fraud as a Service
  - All elements of gathering and using the data also have sales channels
  - Services to test card status, credential validation, phishing, customer contact are all available for a price



## Credential Reuse / Credential Stuffing



People use the same username and password across multiple sites

Threat actors obtain these credentials from various breaches

Use electronic tools like bots to automatically login using these credentials to see where they work

Use the info to commit fraud or sell the info

80% of hacking related breaches involve weak or previously stolen credentials

## Faster Payments are Becoming the Norm



### Real Time Payments

- Once payment is authorized, it cannot be undone
- Know who you are paying
- Don't do business transactions via P2P
- Keep up to date

# Passwords

- Nobody likes creating, managing and changing passwords
- Hackers can purchase tools and algorithms to crack them if they're not long and strong
- Passwords should be:
  - Longer
  - Stronger
  - Don't use info readily available on your social media pages (kid's or pet names)
  - Don't reuse passwords ESPECIALLY for financial sites
  - Don't share passwords
  - Use upper case letters, lower case letters, numbers, special characters



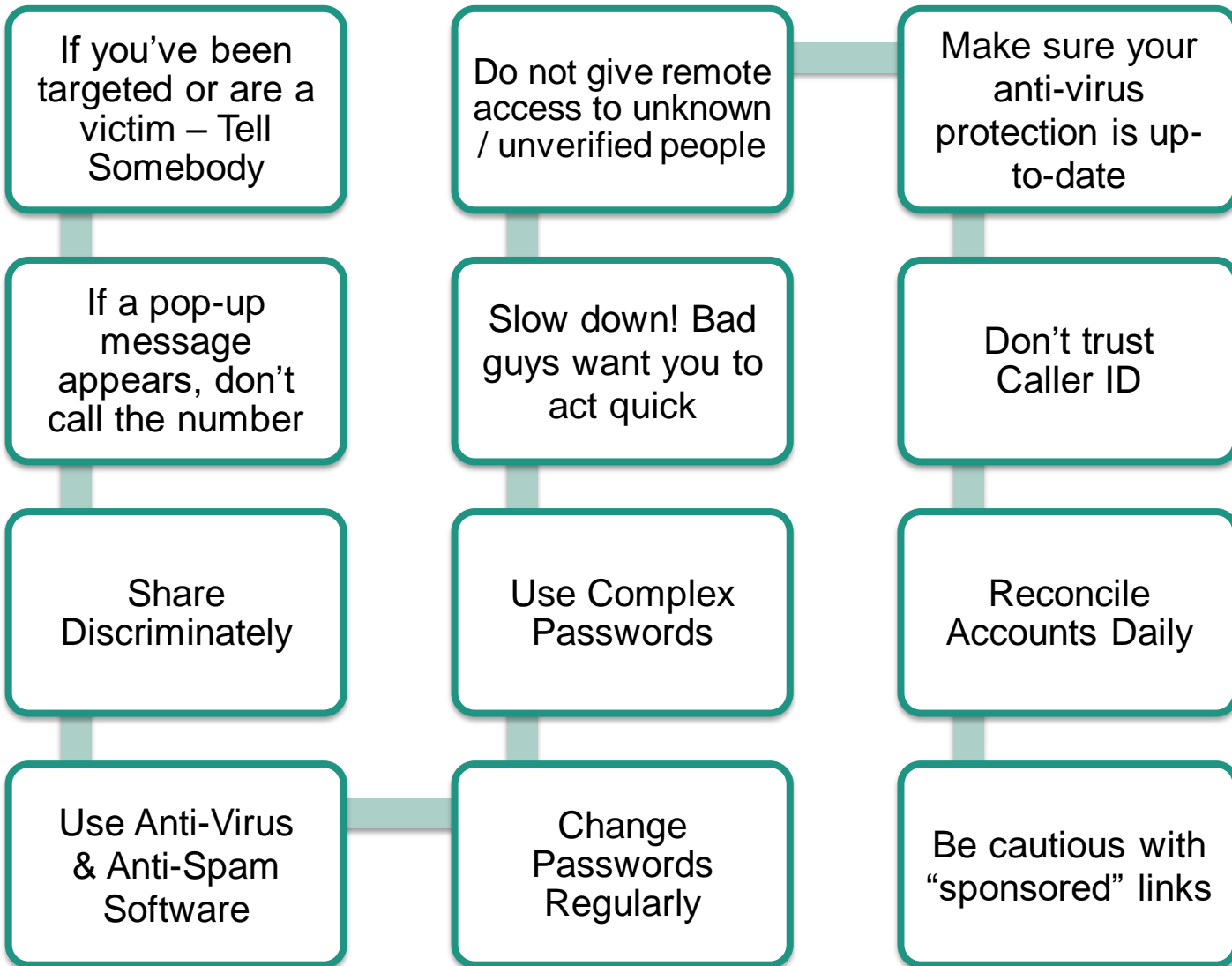


# Passwords

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case aplhabets	Mixed numbers, Lower and Upper case aplhabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years



# Customer Best Practices



## If you are a Victim

- The sooner you can notify the bank, the sooner we can try and retrieve funds
- Contact your local police department. This can help with recovery and insurance claims
- Keep all original documentation, emails, screen shots
- Immediately change all passwords related to financial sites / systems
- Expect additional attempts,. Scammers Often share / sell their victim database info

# Disclosures

- This presentation is for informational and educational purposes only. Nothing herein should be considered or relied upon as legal advice. The author assumes no responsibility or liability for the specific applicability of the information provided. Please consult your own legal counsel for any legal advice.
- Some products and services may be provided through subsidiaries or affiliates of M&T Bank.
- Visa is a registered trademark of Visa International Service Association.
- Unless otherwise specified, all advertised offers and terms and conditions of accounts and services are subject to change at any time without notice. After an account is opened or service begins, it is subject to its features, conditions and terms, which are subject to change at any time in accordance with applicable laws and agreements. Please contact an M&T representative for full details.

## **Contact Info**

*Leigh Balcom, CFE*

[Lbalcom@mtb.com](mailto:Lbalcom@mtb.com)

716-343-6371