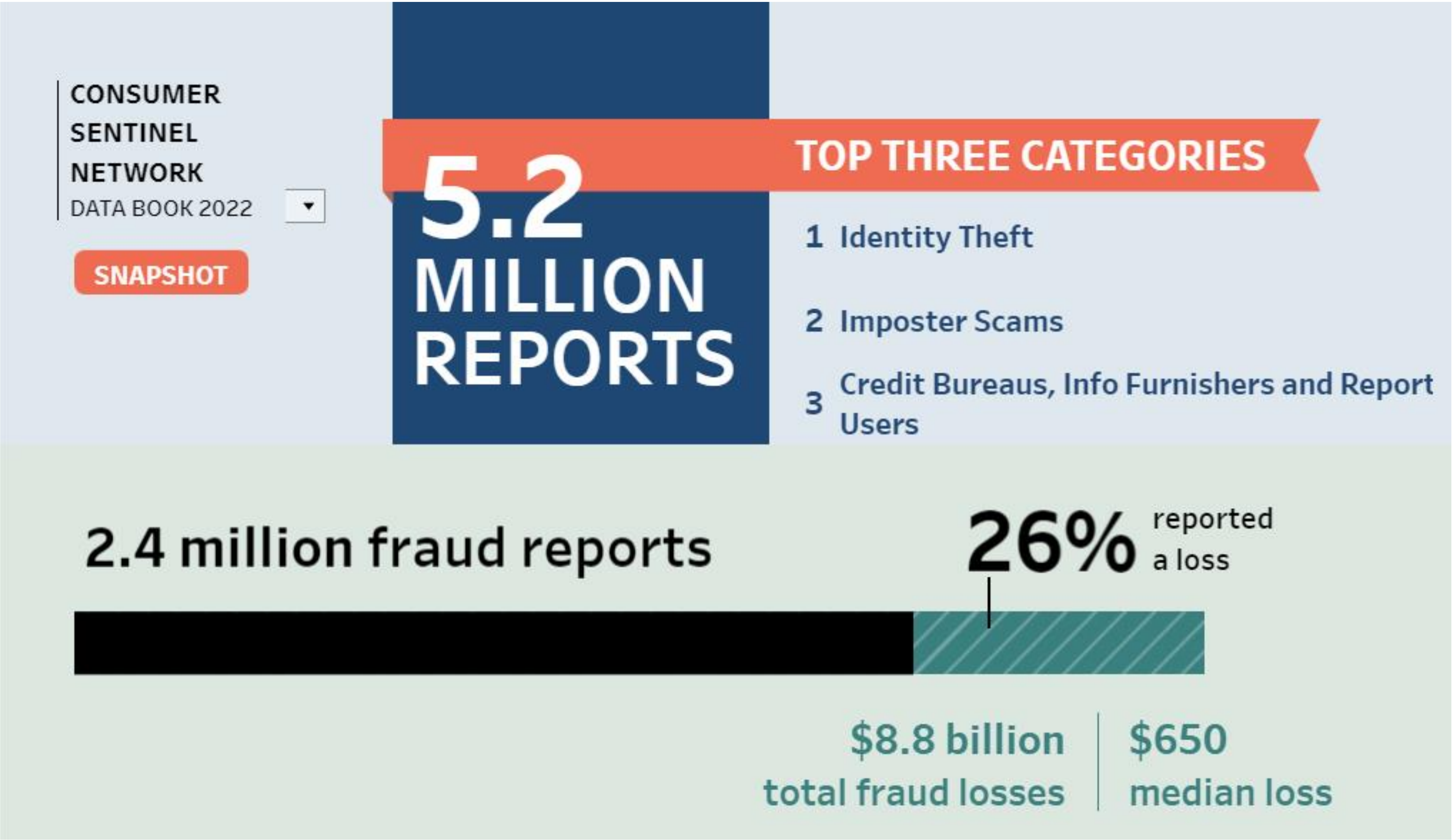
Hilton Head Island Computer Club

HHICC

Members Helping Members Learn Technology Since 1989

Digital Safety Basics

March 27, 2023



CONSUMER
SENTINEL
NETWORK
DATA BOOK 2022 ▾

SNAPSHOT

5.2 MILLION REPORTS

TOP THREE CATEGORIES

1 Identity Theft

2 Imposter Scams

3 Credit Bureaus, Info Furnishers and Report Users

2.4 million fraud reports

26% reported a loss

$8.8 billion total fraud losses

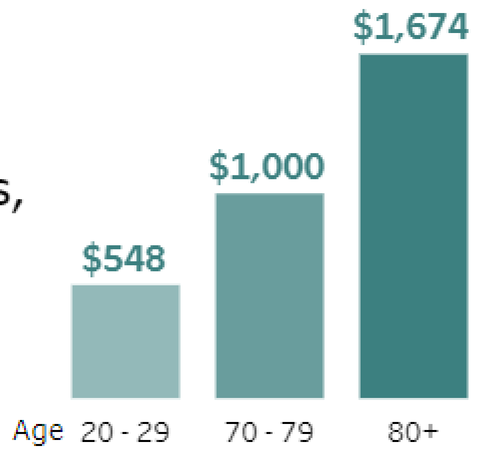
$650 median loss

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

43%
Age 20-29

23%
Age 70-79

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



Imposter Scams

ABOUT
1 in 5 PEOPLE
LOST MONEY

$2.667 billion reported lost

$1,000 median loss

Data as of December 31, 2022

Identity Theft Reports

13% ↑
Credit card new account fraud

88% ↓
Government Benefits Applied For\Received

FEDERAL TRADE COMMISSION • ftc.gov/data

Top 10 Fraud Categories

Rank	Category	# of Reports	% Reporting $ Loss	Total $ Loss	Median $ Loss
1	Imposter Scams	725,989	22%	$2,666.7M	$1,000
2	Online Shopping and Negative Reviews	327,000	47%	$358.1M	$180
3	Prizes, Sweepstakes and Lotteries	143,132	13%	$301.9M	$907
4	Investment Related	104,703	74%	$3,820.0M	$5,000
5	Business and Job Opportunities	92,723	32%	$367.4M	$2,000
6	Internet Services	90,748	5%	$28.5M	$300
7	Telephone and Mobile Services	89,288	9%	$20.9M	$200
8	Health Care	68,496	7%	$16.6M	$258
9	Travel, Vacations and Timeshare Plans	62,445	17%	$103.6M	$1,259
10	Foreign Money Offers and Fake Check Scams	40,903	32%	$123.6M	$2,000

Identity Theft Types

Rank	Theft Type	# of Reports
1	Credit Card Fraud	441,822
2	Other Identity Theft	326,590
3	Bank Fraud	156,099
4	Loan or Lease Fraud	153,547
5	Employment or Tax-Related Fraud	103,402
6	Phone or Utilities Fraud	77,284
7	Government Documents or Benefits Fraud	57,877

We are all experiencing attempted scams

- Imposter Scammers Are Everywhere (trying to earn a living!)
  - Phone Calls
  - Emails
  - Texts
  - Social Media (Facebook, TikTok, etc.)
- They are trying to get information about you that they can sell
  - Credit Card info
  - Bank Account info
  - Social Security and Birth Date
  - Account Sign In Information
- Or they are trying to get you to send them money

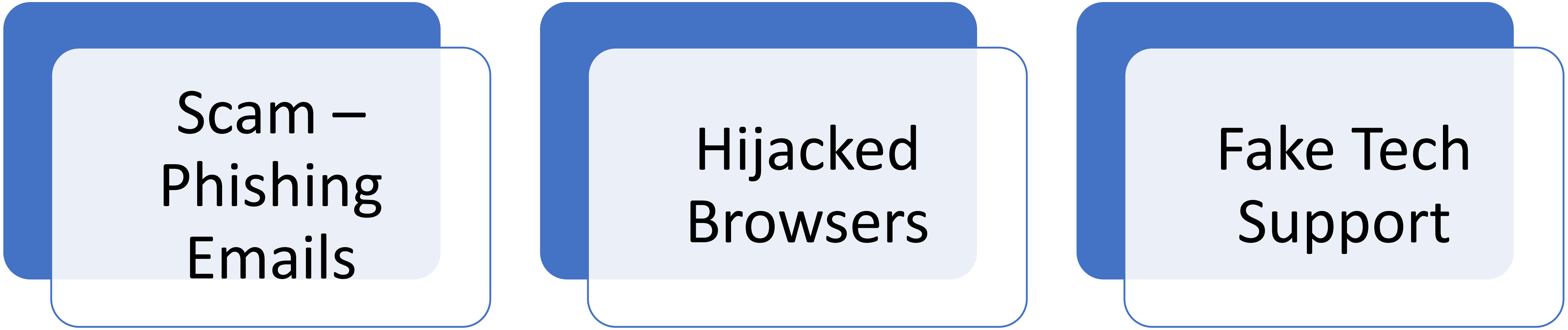
Who are “they”

- Individuals trying to earn a living by selling personal information on the dark web. (credit card info about $2)
- Small groups trying to do Identity Theft by gaining your personal information and opening accounts or making purchases in your name
- Organizations trying to get you to send them money through personal contact (tech support scam, romance scam, investment scam)

Individuals in any place where there is internet service

Groups in poorer countries with strong tech training: Philippines, India, Nigeria, etc…..

What we see the most:

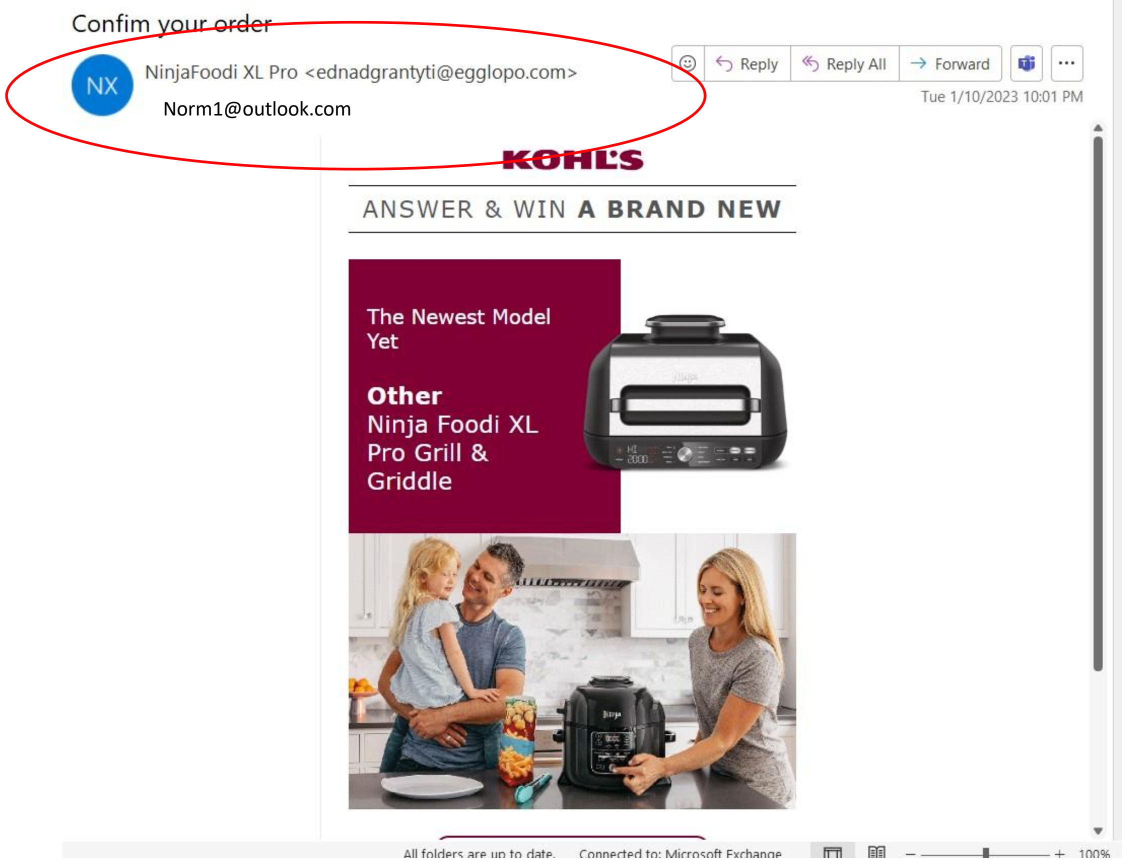


Scam – Phishing Emails

Hijacked Browsers

Fake Tech Support

Scam – Phishing Emails



Confim your order

NX NinjaFoodi XL Pro <ednadgrantyti@egglopo.com>

Norm1@outlook.com

Tue 1/10/2023 10:01 PM

KOHL'S

ANSWER & WIN **A BRAND NEW**

The Newest Model Yet

Other
Ninja Foodi XL Pro Grill & Griddle

All folders are up to date. Connected to: Microsoft Exchange

Check the senders Domain

- @xxxxx.xxx
- If it’s not a *company.com*, spelled correctly, do not trust it

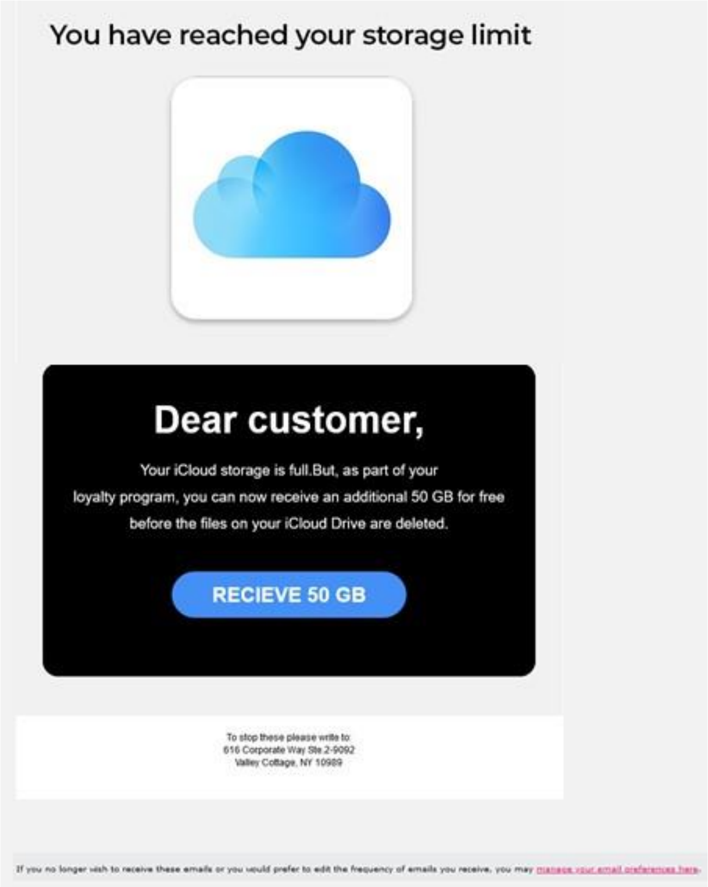
If you don’t trust it, DO NOT Unsubscribe!!!

- Move the email to your junk
- Also, you can go to your mail provider settings and block the domain

Spear Phishing

- Information about you is used to get you to respond
- Social Media info used to send you a message (phone, text, email) that is personalized to your situation

  (Grandson Joey needs help)
- One of your account usernames is on the dark web.



You have reached your storage limit

Dear customer,

Your iCloud storage is full.But, as part of your loyalty program, you can now receive an additional 50 GB for free before the files on your iCloud Drive are deleted.

To stop these please write to:
616 Corporate Way Ste 2-9092
Valley Cottage, NY 10989

If you no longer wish to receive these emails or you would prefer to edit the frequency of emails you receive, you may manage your email preferences here.

When you click, you are asked to log into your Apple account, then give your credit card to purchase more space.

The Phisher now has your Apple account ID and your credit card and whatever cash you paid!!

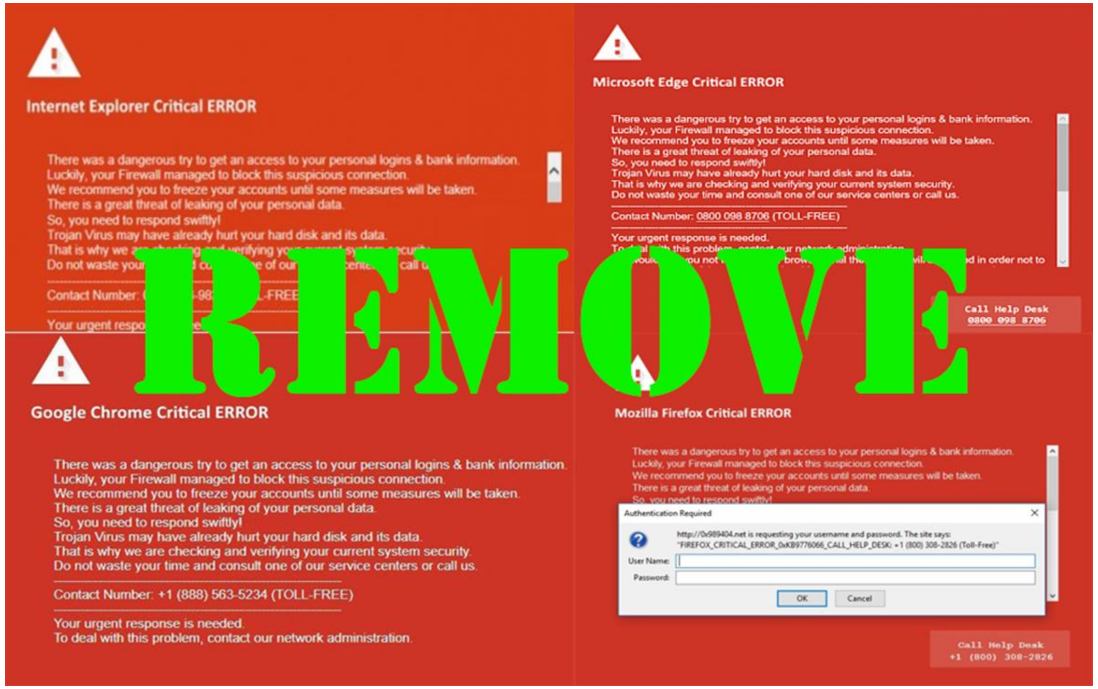
Whale Phishing

- A lot of information is found out about an individual and is used to get something very valuable.
  - People with corporate positions
  - People with means

  - Pastors
  - Church Treasurers
  - Club leaders

If there is any question, investigate before responding.

Hijacked Browser



Internet Explorer Critical ERROR

There was a dangerous try to get an access to your personal logins & bank information.
Luckily, your Firewall managed to block this suspicious connection.
We recommend you to freeze your accounts until some measures will be taken.
There is a great threat of leaking of your personal data.
So, you need to respond swiftly!
Trojan Virus may have already hurt your hard disk and its data.
That is why we [illegible] your [illegible] security.
Do not waste your [illegible] c[illegible]e of our [illegible] cente[illegible] call u[illegible]

Contact Number: ([illegible]-98[illegible]L-FREE

Your urgent respo[illegible]e[illegible]

Microsoft Edge Critical ERROR

There was a dangerous try to get an access to your personal logins & bank information.
Luckily, your Firewall managed to block this suspicious connection.
We recommend you to freeze your accounts until some measures will be taken.
There is a great threat of leaking of your personal data.
So, you need to respond swiftly!
Trojan Virus may have already hurt your hard disk and its data.
That is why we are checking and verifying your current system security.
Do not waste your time and consult one of our service centers or call us.

Contact Number: 0800 098 8706 (TOLL-FREE)

Your urgent response is needed.
To [illegible]al with this proble[illegible] our network administration
[illegible]ould [illegible]ou not [illegible] brow[illegible] the [illegible] wil[illegible]d in order not to

Call Help Desk
0800 098 8706

Google Chrome Critical ERROR

There was a dangerous try to get an access to your personal logins & bank information.
Luckily, your Firewall managed to block this suspicious connection.
We recommend you to freeze your accounts until some measures will be taken.
There is a great threat of leaking of your personal data.
So, you need to respond swiftly!
Trojan Virus may have already hurt your hard disk and its data.
That is why we are checking and verifying your current system security.
Do not waste your time and consult one of our service centers or call us.

Contact Number: +1 (888) 563-5234 (TOLL-FREE)

Your urgent response is needed.
To deal with this problem, contact our network administration.

Mozilla Firefox Critical ERROR

There was a dangerous try to get an access to your personal logins & bank information.
Luckily, your Firewall managed to block this suspicious connection.
We recommend you to freeze your accounts until some measures will be taken.
There is a great threat of leaking of your personal data.
So, you need to respond swiftly!

Authentication Required

http://0x989404.net is requesting your username and password. The site says: "FIREFOX_CRITICAL_ERROR_0xKB9776066_CALL_HELP_DESK: +1 (800) 308-2826 (Toll-Free)"

User Name:

Password:

Call Help Desk
+1 (800) 308-2826

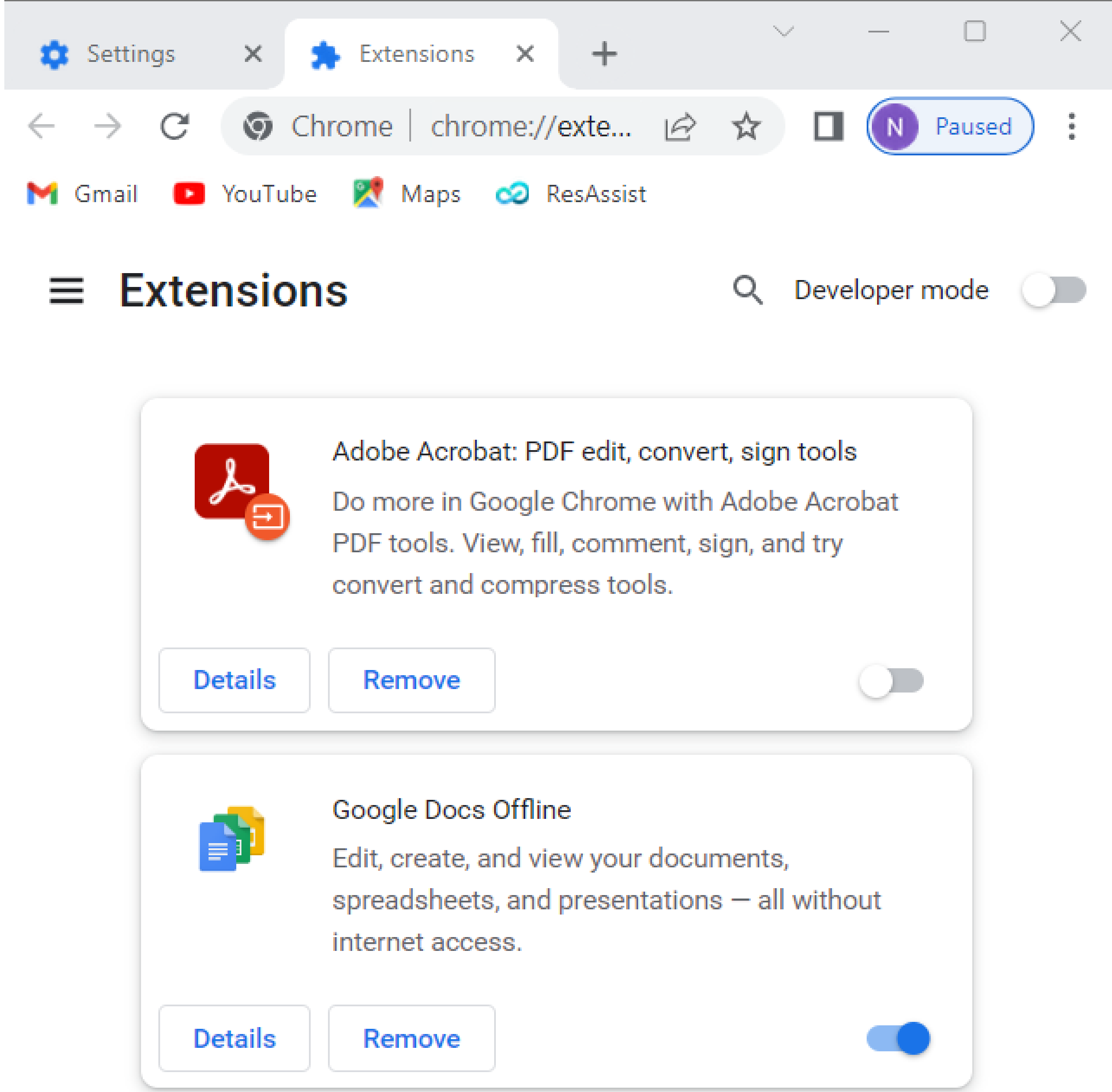
- You go to a website and all of a sudden, your screen is locked with some big warning message and a phone number to call for help! **Don’t call the number!**
- Do not click anywhere in the browser screen.
- Go to task manager and close every occurrence of the browser.
- Reboot – you should be good

Fake Tech Support

- Warning message on a website with a phone number to call
- Searching the web for a phone number to call for tech help
- Pop-Up message or notification
- Unsolicited phone call offering help

- In every case, just say no!
  - Do not let anyone take over your computer unless you **know certainly** that they are a “trusted provider”
  - Do not purchase an annual contract.

Fake System Warnings can come from your Browser Extensions.
In Chrome go to Settings and Select Extensions.
- Be sure you want them all



Extensions

Developer mode

Adobe Acrobat: PDF edit, convert, sign tools

Do more in Google Chrome with Adobe Acrobat PDF tools. View, fill, comment, sign, and try convert and compress tools.

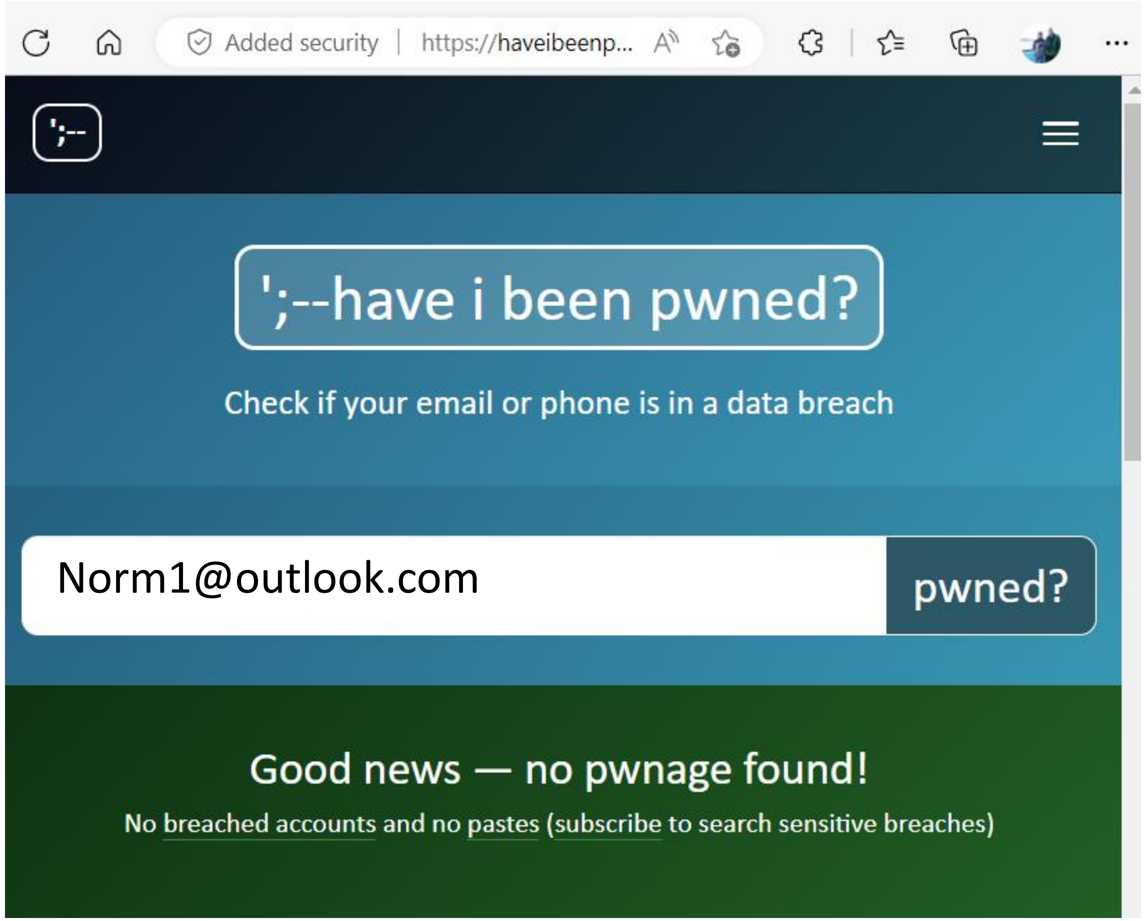
Google Docs Offline

Edit, create, and view your documents, spreadsheets, and presentations — all without internet access.

Protecting Your Online Accounts

- Username and Password management
- Two Step Authentication
- Beware of Mobile Phone Thefts

haveibeenpwned.com

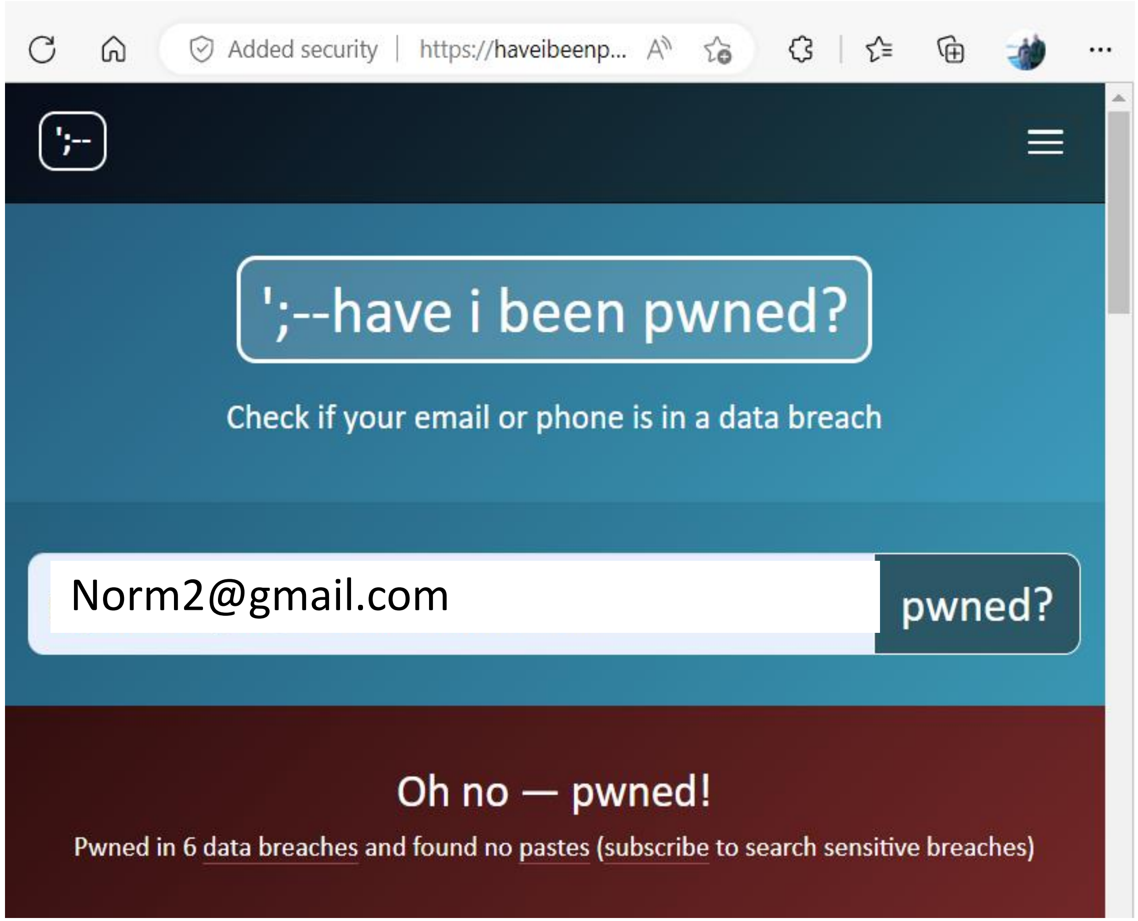


Check if your email or phone is in a data breach

Norm1@outlook.com

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

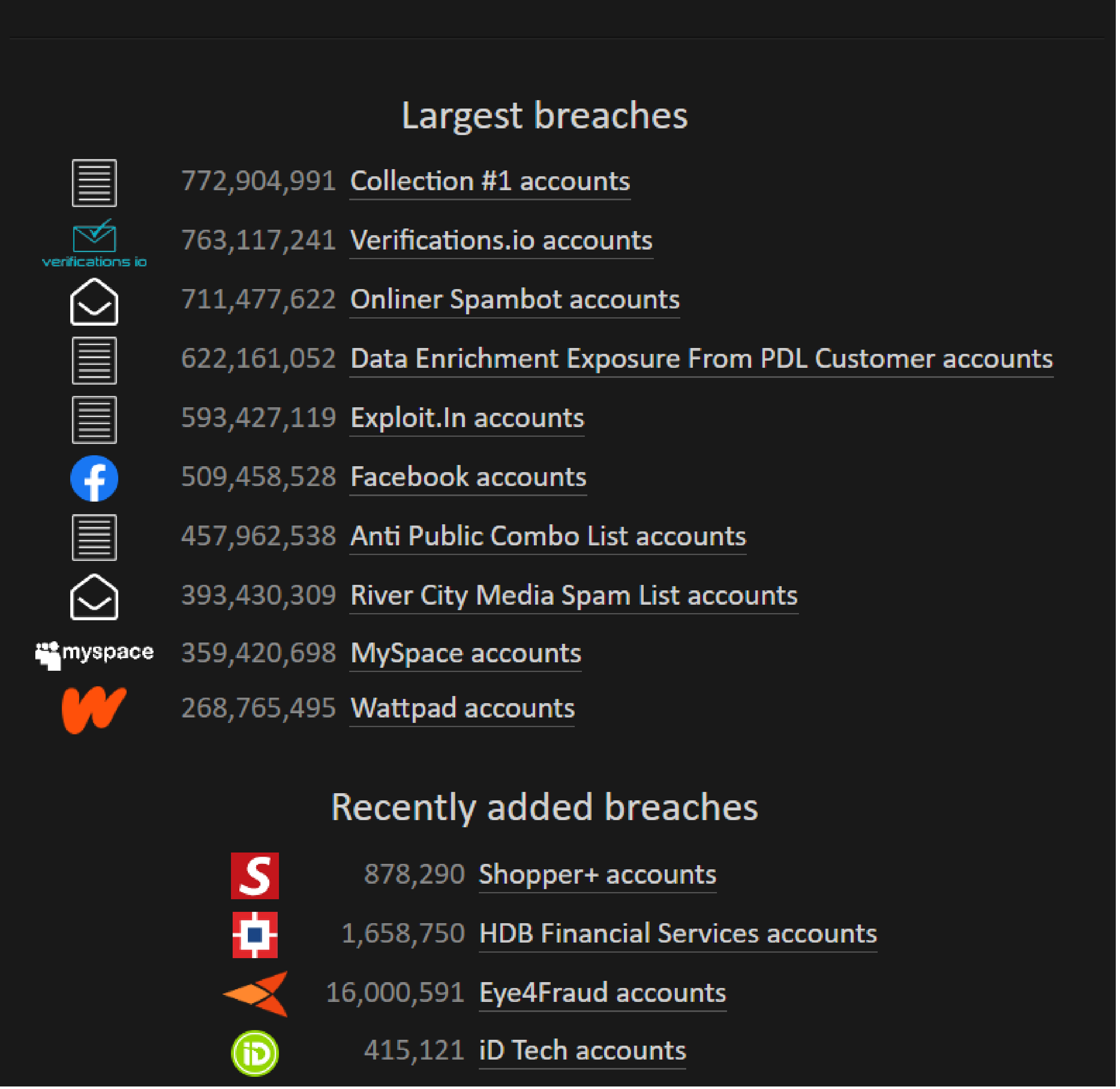


Check if your email or phone is in a data breach

Norm2@gmail.com

Oh no — pwned!

Pwned in 6 data breaches and found no pastes (subscribe to search sensitive breaches)

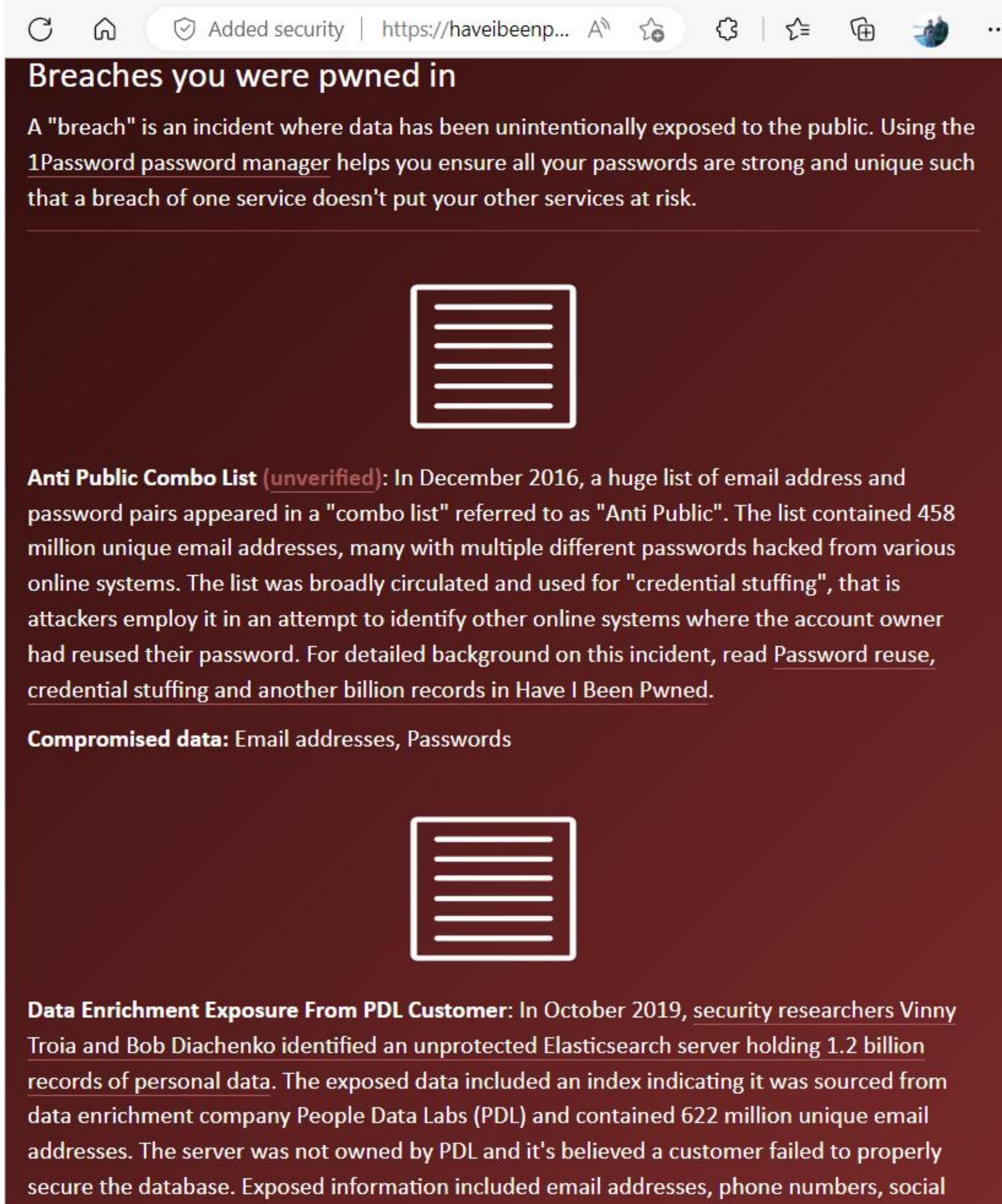


Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
622,161,052	Data Enrichment Exposure From PDL Customer accounts
593,427,119	Exploit.In accounts
509,458,528	Facebook accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
268,765,495	Wattpad accounts

Recently added breaches

878,290	Shopper+ accounts
1,658,750	HDB Financial Services accounts
16,000,591	Eye4Fraud accounts
415,121	iD Tech accounts



Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Anti Public Combo List (unverified): In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.

Compromised data: Email addresses, Passwords

Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social

Some Simple Rules

- Do not use a password more than once
- When you chose a password, do it uniquely – changing a single letter or symbol makes it easy to remember, but they are “cracked” by machines that are good at guessing and will start with one they know you used.
- Have a way to store and retrieve all of the username and passwords for all of your different accounts.
  - 1.Password Manager, 2. Document stored in the cloud (iCloud, Google Cloud, OneDrive) – should be encrypted, or 3. Written in a notebook or password book stored not on your physical desktop.

Identity Theft Insurance

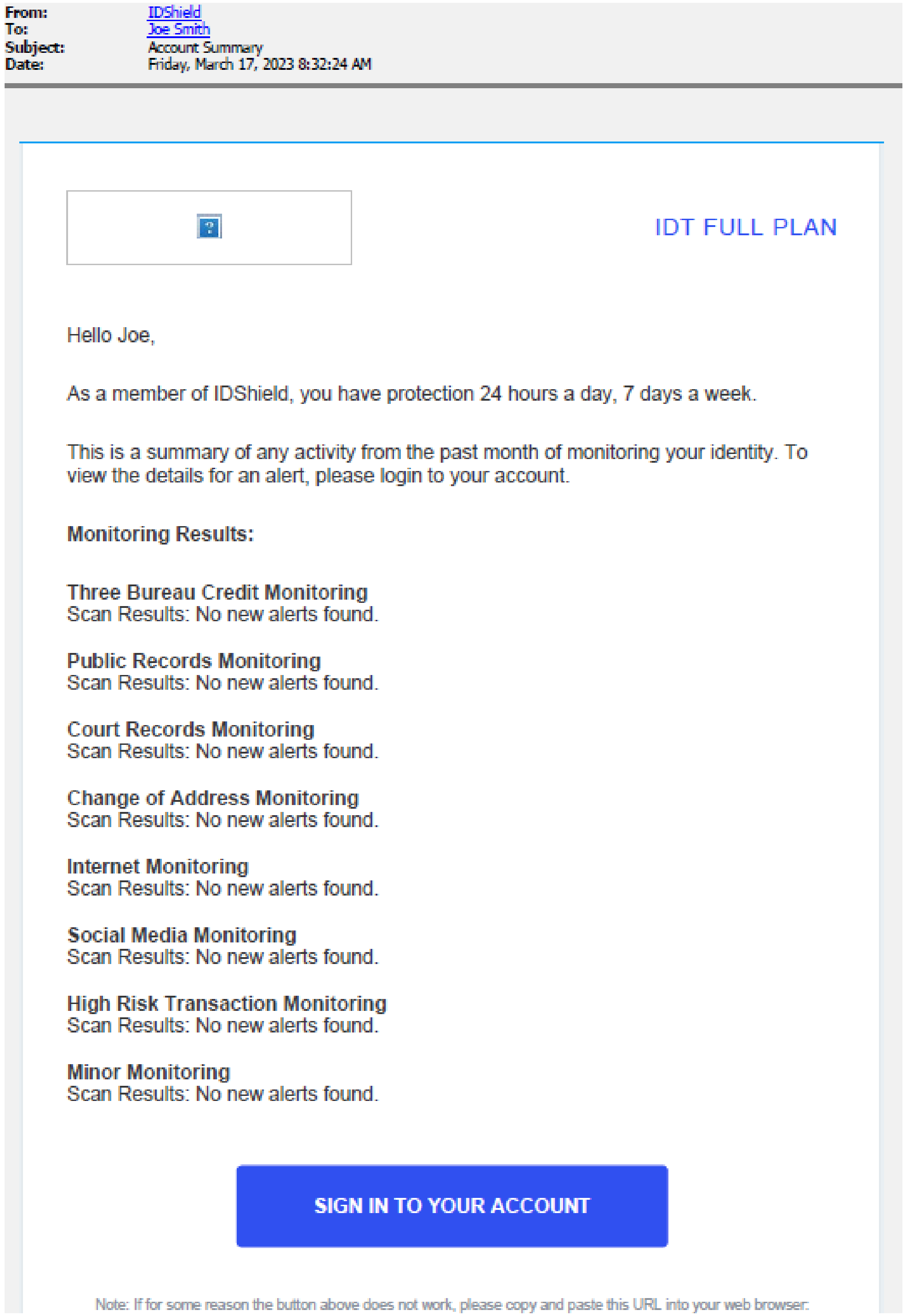
US News 2023 list

- **#1 IdentityForce** – Best Identity Theft Protection Service of 2023
- **#2 IDShield** – Best for Identity Recovery Assistance
- **#3 (tie) Aura**
- **#3 (tie) Zander** – Best Budget Identity theft Protection Service
- **#5 (tie) Identity Guard**
- **#5 (tie) ID Watchdog** – Best for Customized Identity Monitoring
- **#7 (tie) ReliaShield**
- **#7 (tie) LifeLock** – Best for Computer and Device Protection
- **#9 (tie) IdentityIQ** – Best for Family Protection
- **#9 (tie) myFICO** – Best for Detailed FICO Scores

ID Shield

Monitors many types of records for changes
Monitors the Dark Web for “information for sale”
Sends details on any alerts
Sends monthly status
Provides Recovery Help and Insurance

(This is not an advertisement!!! Just happens to be what the presenter uses)



From: IDShield
To: Joe Smith
Subject: Account Summary
Date: Friday, March 17, 2023 8:32:24 AM

IDT FULL PLAN

Hello Joe,

As a member of IDShield, you have protection 24 hours a day, 7 days a week.

This is a summary of any activity from the past month of monitoring your identity. To view the details for an alert, please login to your account.

Monitoring Results:

Three Bureau Credit Monitoring
Scan Results: No new alerts found.

Public Records Monitoring
Scan Results: No new alerts found.

Court Records Monitoring
Scan Results: No new alerts found.

Change of Address Monitoring
Scan Results: No new alerts found.

Internet Monitoring
Scan Results: No new alerts found.

Social Media Monitoring
Scan Results: No new alerts found.

High Risk Transaction Monitoring
Scan Results: No new alerts found.

Minor Monitoring
Scan Results: No new alerts found.

Note: If for some reason the button above does not work, please copy and paste this URL into your web browser:

Never Stop Learning

Visit the Resource Center!

If you have questions about a strange Notification, email or social media message, call or come for help. We learn while we help you and can share what the bad guys are up to!