

Staying Safe in a Connected World

Protecting Yourself Online and Offline

Agenda

- **Who is the guy talking... About Vinodh**
- **Common Scams | Who are targeted**
- **Some Stats**
- **Spotting Issues**
- **Smart Choices**
- **Internet Safety & Secure Browsing**
- **Reporting & Getting help**
- **Q&A**

Common Scams

How to Spot them

Phishing

- **Phone: IRS, Medicare, Car Warranty**
- **Email: Bank alerts, prize winnings, confirmed orders**
- **Door-to-door: Fake contractors, charities**
 - **Urgent or threatening tone**
 - **Spelling mistakes**
 - **Suspicious links/attachments**

Investment

- **Guaranteed returns**
- **Pressure to act fast**
- **Unlicensed sellers**
- **Check with FINRA/SEC**

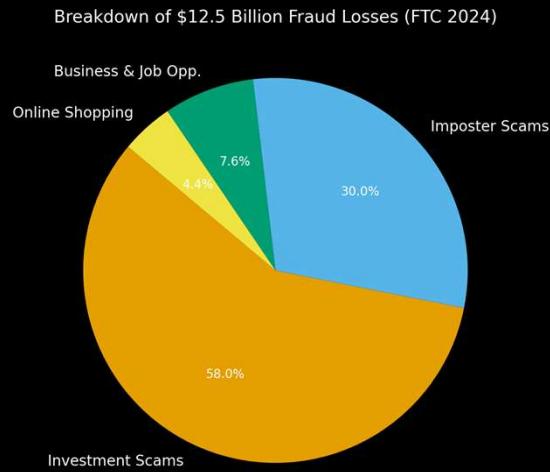
Rule: Don't click, don't reply, verify first

Who are Targeted

EVERYONE!

- **Seen as trusting**
- **Financially Stable**
- **Less Tech-Savvy**
- **Random Targets**
- **Thousands Targeted in Houston**

2024 Stats



https://www.ftc.gov/system/files/ftc_gov/images/csn-scammy-snapshot-2024.png

Snapshot:

- **2.6 million fraud reports filed**
- **\$12.5 billion reported lost (25% increase from 2023)**
- **1 in 3 people who reported scams lost money**

Top Scams:

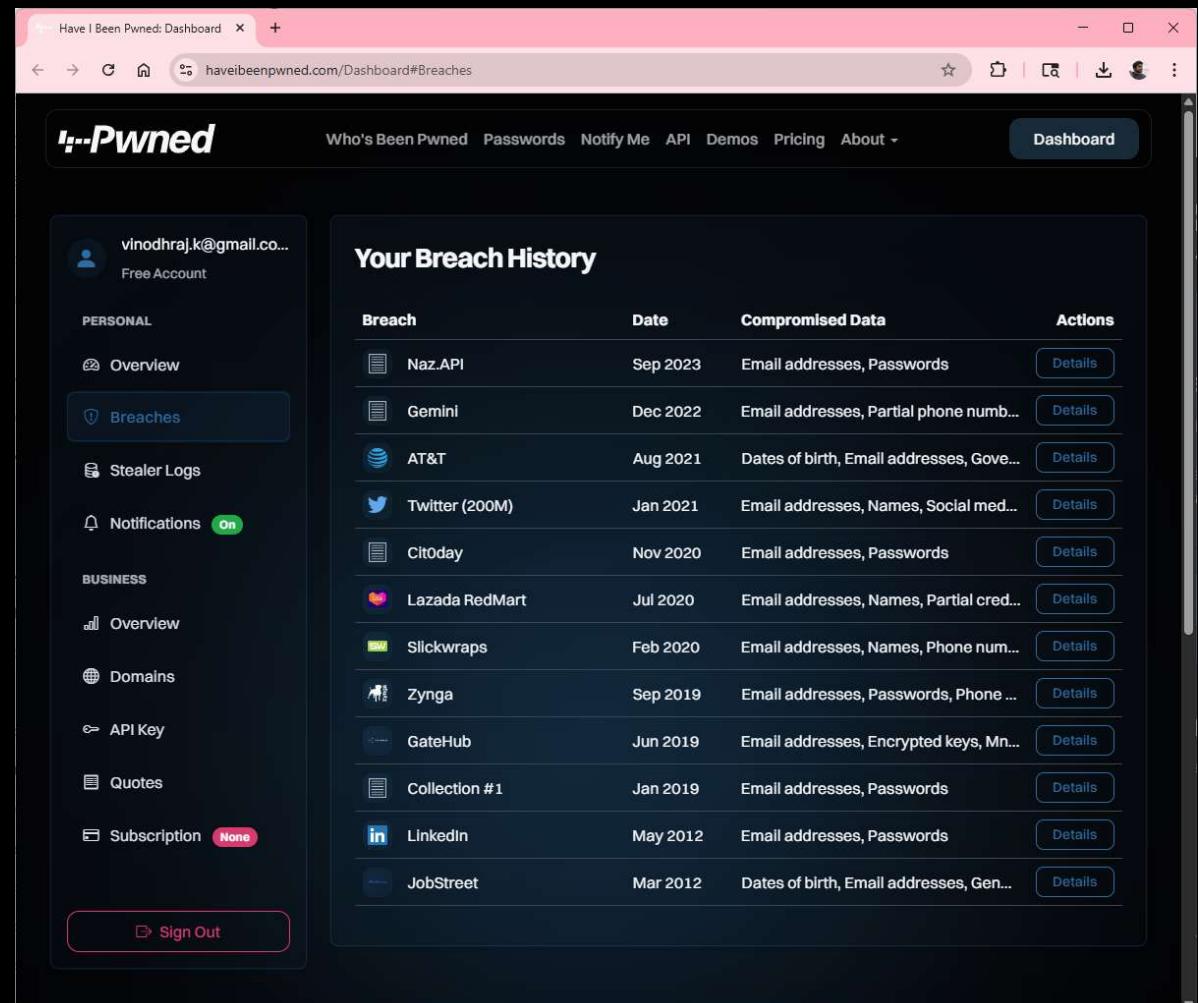
- **Imposters**
- **Online shopping & reviews**
- **Business & job opportunities**
- **Investments**
- **Internet services**

Other Key Facts:

- **Job scams: \$501M losses in 2024**
- **Phone calls: \$1,500 median loss**
- **Social media scams: \$1.9B total loss**
- **Email scams: 372,000 reports**

**Yes, I have
been
breached.**

haveibeenpwned.com



The screenshot shows the Have I Been Pwned dashboard. The left sidebar, titled 'Pwned', lists 'PERSONAL' and 'BUSINESS' sections. Under PERSONAL, 'Overview' and 'Breaches' are listed, with 'Breaches' being the active tab. Under BUSINESS, 'Overview', 'Domains', 'API Key', 'Quotes', and 'Subscription' (None) are listed. The main content area, titled 'Your Breach History', displays a table of 15 data breaches. Each row includes the breach name, date, compromised data types, and a 'Details' button. The breaches listed are: Naz.API (Sep 2023, Email addresses, Passwords), Gemini (Dec 2022, Email addresses, Partial phone numb...), AT&T (Aug 2021, Dates of birth, Email addresses, Gove...), Twitter (200M) (Jan 2021, Email addresses, Names, Social med...), Cl0day (Nov 2020, Email addresses, Passwords), Lazada RedMart (Jul 2020, Email addresses, Names, Partial cred...), Slickwraps (Feb 2020, Email addresses, Names, Phone num...), Zynga (Sep 2019, Email addresses, Passwords, Phone ...), GateHub (Jun 2019, Email addresses, Encrypted keys, Mn...), Collection #1 (Jan 2019, Email addresses, Passwords), LinkedIn (May 2012, Email addresses, Passwords), and JobStreet (Mar 2012, Dates of birth, Email addresses, Gen...).

Breach	Date	Compromised Data	Actions
Naz.API	Sep 2023	Email addresses, Passwords	Details
Gemini	Dec 2022	Email addresses, Partial phone numb...	Details
AT&T	Aug 2021	Dates of birth, Email addresses, Gove...	Details
Twitter (200M)	Jan 2021	Email addresses, Names, Social med...	Details
Cl0day	Nov 2020	Email addresses, Passwords	Details
Lazada RedMart	Jul 2020	Email addresses, Names, Partial cred...	Details
Slickwraps	Feb 2020	Email addresses, Names, Phone num...	Details
Zynga	Sep 2019	Email addresses, Passwords, Phone ...	Details
GateHub	Jun 2019	Email addresses, Encrypted keys, Mn...	Details
Collection #1	Jan 2019	Email addresses, Passwords	Details
LinkedIn	May 2012	Email addresses, Passwords	Details
JobStreet	Mar 2012	Dates of birth, Email addresses, Gen...	Details

What can I do NOW

- **Do not Install/Review unknown Apps on the Phone**
- **Block overseas usage of Cards**
- **Create alerts on Banking Transactions**
- **Do not share OTPs PINs**
- **Strong Passwords**
 - **If you must use a password**
 - **Choose a Phrase – minimum 12 characters**
 - **Complicate it**
 - **Example: !L0veT3x@su\$#**
- **Credit Freezes**
 - **stops anyone from opening new accounts in your name**

What tools can I use?



- **Passwords Managers**
 - Helps Auto Generate Strong Passwords & remember them
 - Notify if passwords have been compromised
 - iPhone: Keychain | Android: Password Manager
- **Use Passkeys**
 - More secure and easier than Passwords
- **Data Monitoring Services**
 - Banks
 - Credit Karma
- **Two Factor Authentications**
 - Apps like Google or Microsoft Authenticator
 - Mobile number

Safe Use of Cards, Online Banking & Protecting Personal Information

- **Use trusted ATMs**
- **Use Credit Cards – They have stronger Fraud Protection**
- **Shield your PIN – Remember it – Do not write it anywhere**
- **Enable two-factor**
- **Only use secure sites (<https://>)**
- **Set up bank alerts**

- **Protect SSN, bank info, passwords**
- **Shred old bills**
- **Use strong passwords**
- **Don't carry all IDs/cards at once**
- **Do not overshare on Social Media**

Internet Safety & Browsing Smart

- **Keep Devices and Browsers updated**
- **Modern Browsers have pop-up blockers, and malware warnings – enable them**
- **Avoid pop-ups & fake alerts [Loads of attractive Ads are out there]**
- **Shop only on secure sites (<https://> + lock)**
- **Use antivirus protection**
- **Avoid entering passwords or banking on public Wi-Fi (airports, coffee shops).**

What to Do if Identity Theft Happens

- **Call your bank/credit card company and place a freeze on the card/account**
- **Report to Authorities**
- **File a police report**
- **Change and Secure Accounts**

Reporting Scams & Staying Informed

- **Houston Police Department**
- **Texas Attorney General Consumer Protection [State]**
- **Federal Trade Commission [Central]**
- **AARP Fraud Watch Helpline [Guidance, Education & Support]**
- [**https://www.texasattorneygeneral.gov/consumer-protection**](https://www.texasattorneygeneral.gov/consumer-protection)
- [**ftc.gov/complaint**](https://www.ftc.gov/complaint)
- **AARP: American Association of Retired Persons**
 - [**https://www.aarp.org/forms/scam-map-form-page/**](https://www.aarp.org/forms/scam-map-form-page/)
 - **1-877-908-3360**

Q & A

Awareness is KEY

**Stay
Safe!**

Thank You!