Day 6 — Email, Phone & Breach Research (Practical)

Goal: check whether an email or phone number appears in public breaches/pastes, gather reputation info, and produce remediation actions for an OSINT report.

Prerequisites

- Browser (Chrome/Firefox)
- PowerShell (Windows) or bash (Linux/macOS)
- `curl` (Linux/macOS) or PowerShell `Invoke-WebRequest`
- `jq` (optional)
- Optional: Truecaller account, Git, Go or WSL if running PhoneInfoga locally

0) Safety & scope reminder

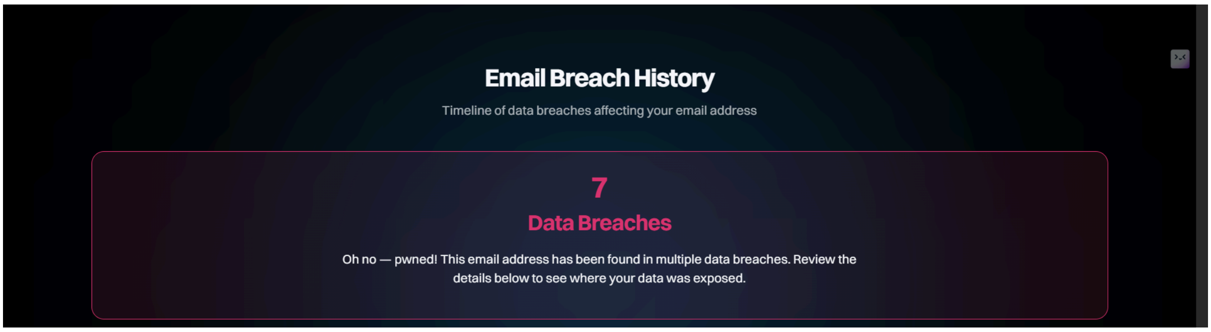
- Only test your own emails/phone numbers or explicit lab accounts.
- Do not attempt to use breached credentials to log into services.
- Treat discovered secrets as sensitive — recommend rotation; do not reuse.

1) Have I Been Pwned (HIBP) — web UI

Why: reliable aggregate of breaches.

Browser steps

1. Open: `https://haveibeenpwned.com/`
2. Enter the **email address** → click **pwned?**
3. If breached, note breach names and exposed data.



Email Breach History

Timeline of data breaches affecting your email address

7

Data Breaches

Oh no — pwned! This email address has been found in multiple data breaches. Review the details below to see where your data was exposed.

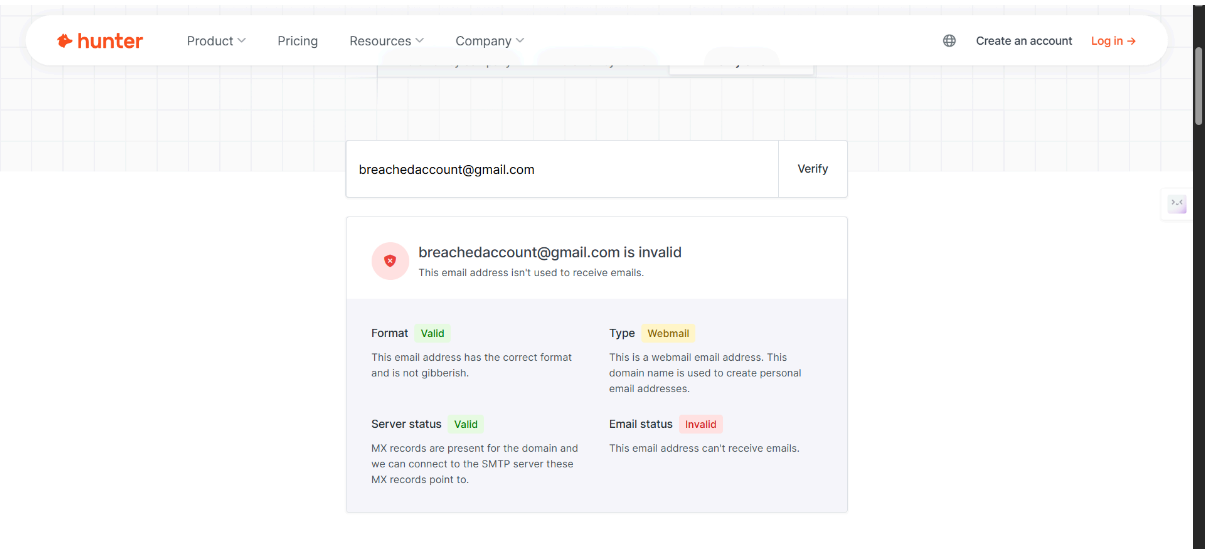
2) Email reputation — EmailRep / Hunter

A. EmailRep (web)

1. Open: `https://emailrep.io`
2. Enter email → view risk score, flags, public links.

B. Hunter (optional)

1. Open: `https://hunter.io`
2. Use the email/domain verifier or search domain patterns.



breachedaccount@gmail.com

breachedaccount@gmail.com is invalid

This email address isn't used to receive emails.

Format Valid

This email address has the correct format and is not gibberish.

Type Webmail

This is a webmail email address. This domain name is used to create personal email addresses.

Server status Valid

MX records are present for the domain and we can connect to the SMTP server these MX records point to.

Email status Invalid

This email address can't receive emails.

3) Search paste sites & public dumps (cautious)

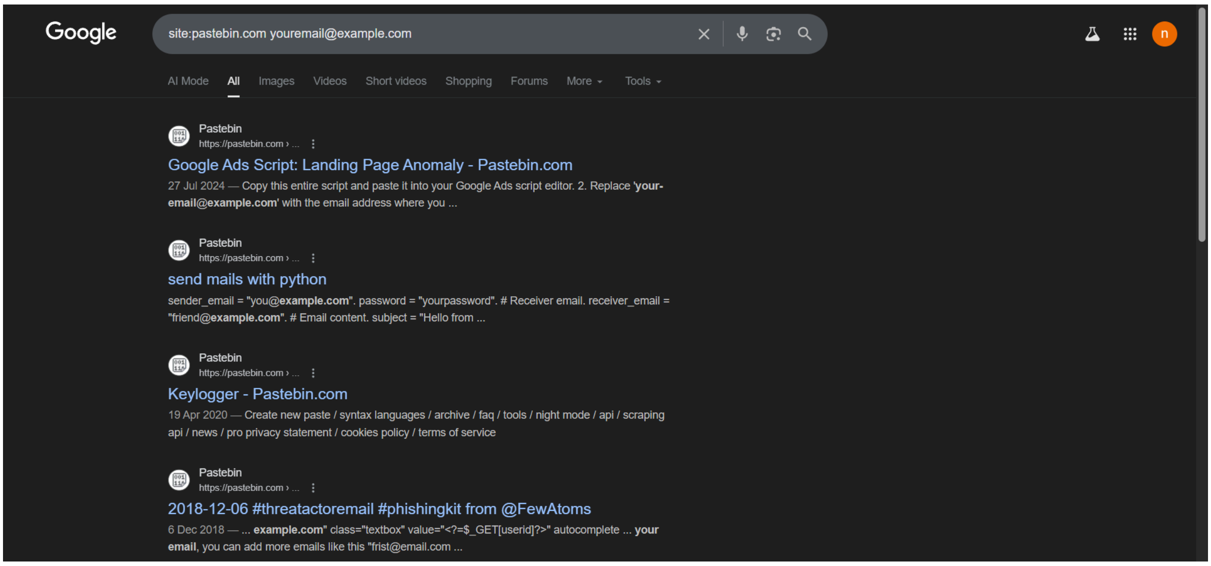
Why: pastes often contain leaked credentials or mentions.

Use Google site searches (do not download attachments)

site:pastebin.com "youremail@example.com"
site:ghostbin.com "youremail@example.com"
site:pastebin.com "yourPasswordInQuotes" # risky — avoid if possible

HIBP Pastes

- Visit: `https://haveibeenpwned.com/Pastes` and enter the email.



Pastebin
https://pastebin.com › ...
Google Ads Script: Landing Page Anomaly - Pastebin.com
27 Jul 2024 — Copy this entire script and paste it into your Google Ads script editor. 2. Replace **'your-email@example.com'** with the email address where you ...

Pastebin
https://pastebin.com › ...
send mails with python
sender_email = "you@**example.com**". password = "yourpassword". # Receiver email. receiver_email = "friend@**example.com**". # Email content. subject = "Hello from ...

Pastebin
https://pastebin.com › ...
Keylogger - Pastebin.com
19 Apr 2020 — Create new paste / syntax languages / archive / faq / tools / night mode / api / scraping api / news / pro privacy statement / cookies policy / terms of service

Pastebin
https://pastebin.com › ...
2018-12-06 #threatactoremail #phishingkit from @FewAtoms
6 Dec 2018 — ... **example.com**" class="textbox" value="<?=$_GET[userid]?>" autocomplete ... **your email**, you can add more emails like this "frist@email.com ...

4) Phone number reconnaissance — PhoneInfoga / Truecaller

Option A: Web (Truecaller) — easiest on Windows

1. Open: `https://www.truecaller.com/` (login may be required)
2. Search number in international format (e.g., `+911234567890`).
3. Screenshot results.

Option B: PhoneInfoga (local)

Clone (one-time)

```
git clone https://github.com/sundowndev/PhoneInfoga.git
cd PhoneInfoga
```

If repo is Go-based (modern):

- Install Go: https://go.dev/dl/

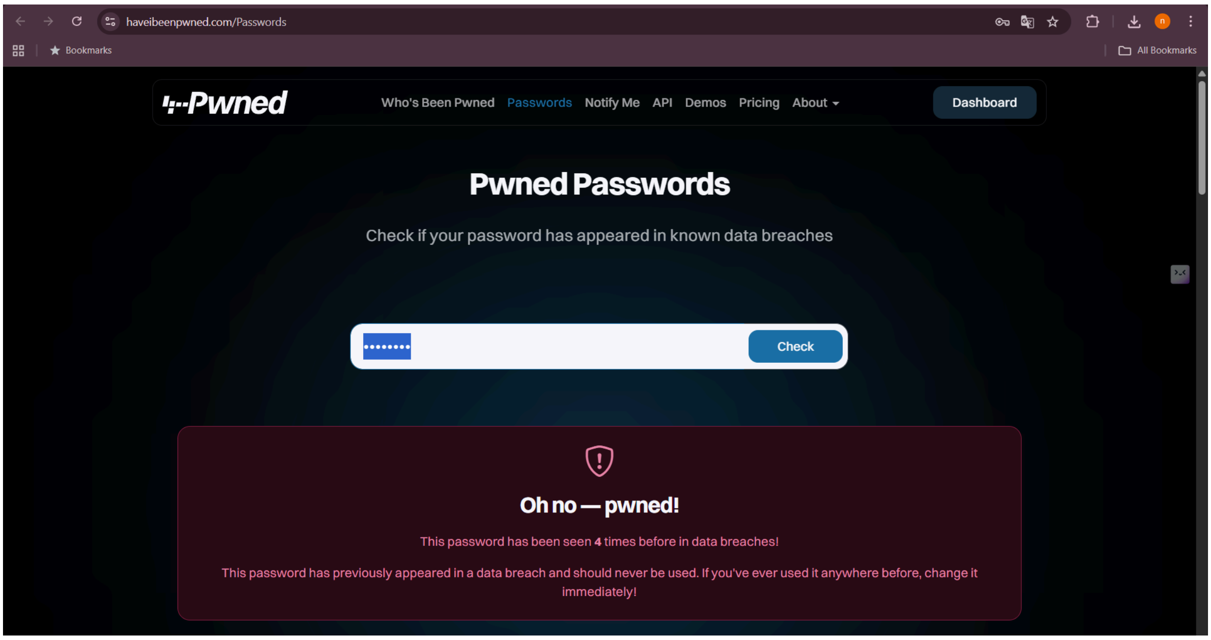
```
# on Windows after installing Go
cd C:\Users\<you>\PhoneInfoga
go build main.go
# run (example)
.\main.exe scan -n "+911234567890" -o
```

5) Check breached passwords exposure (HIBP k-anonymity) — optional, local

Only for passwords you own.

Quick web method (fast)

- Open: `https://haveibeenpwned.com/Passwords` and paste the password (you own) → click **pwned**



Pwned Passwords

Check if your password has appeared in known data breaches

••••••••

Oh no — pwned!

This password has been seen **4** times before in data breaches!

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it immediately!