

# Information Security

**What do I need to know in 2021?**

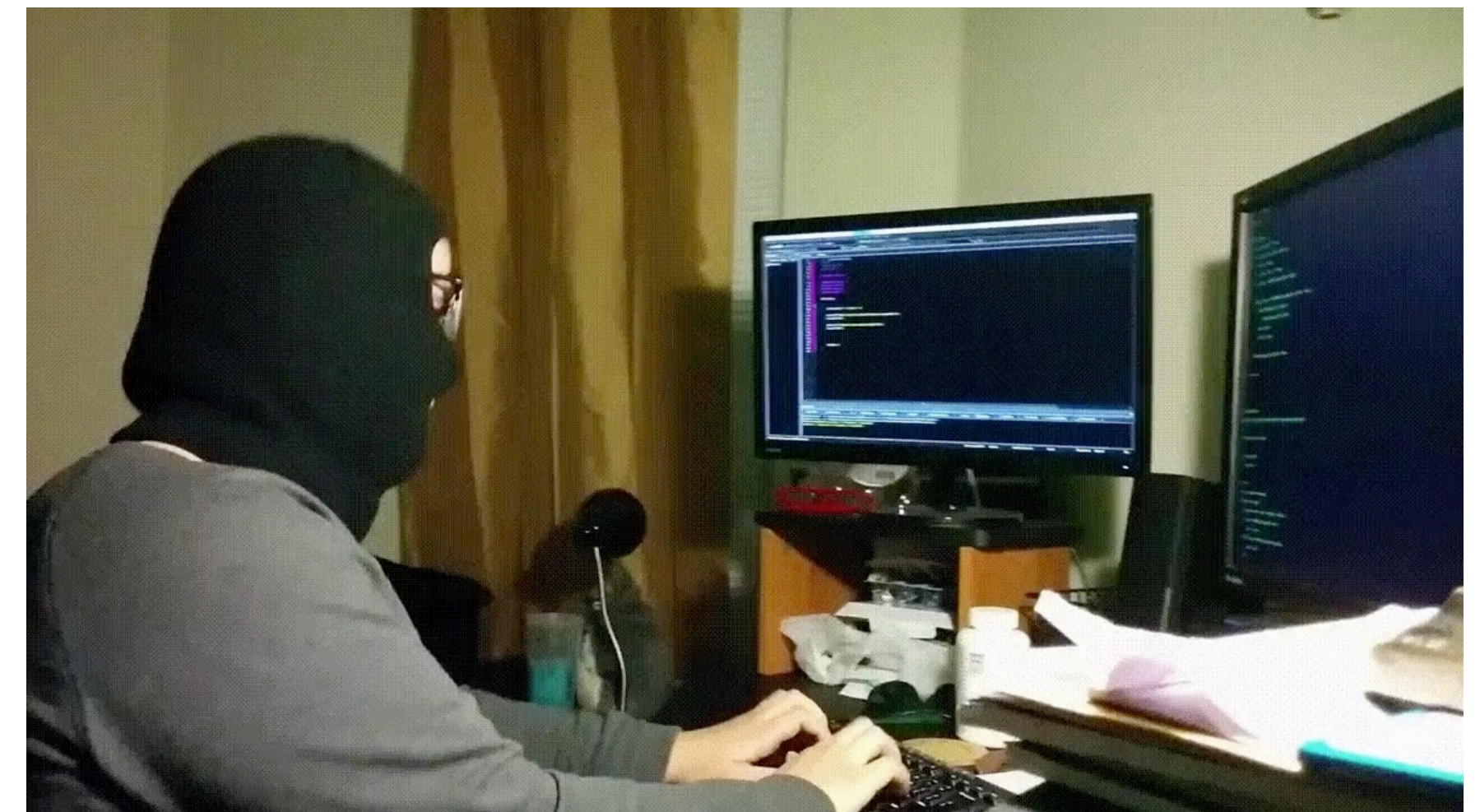
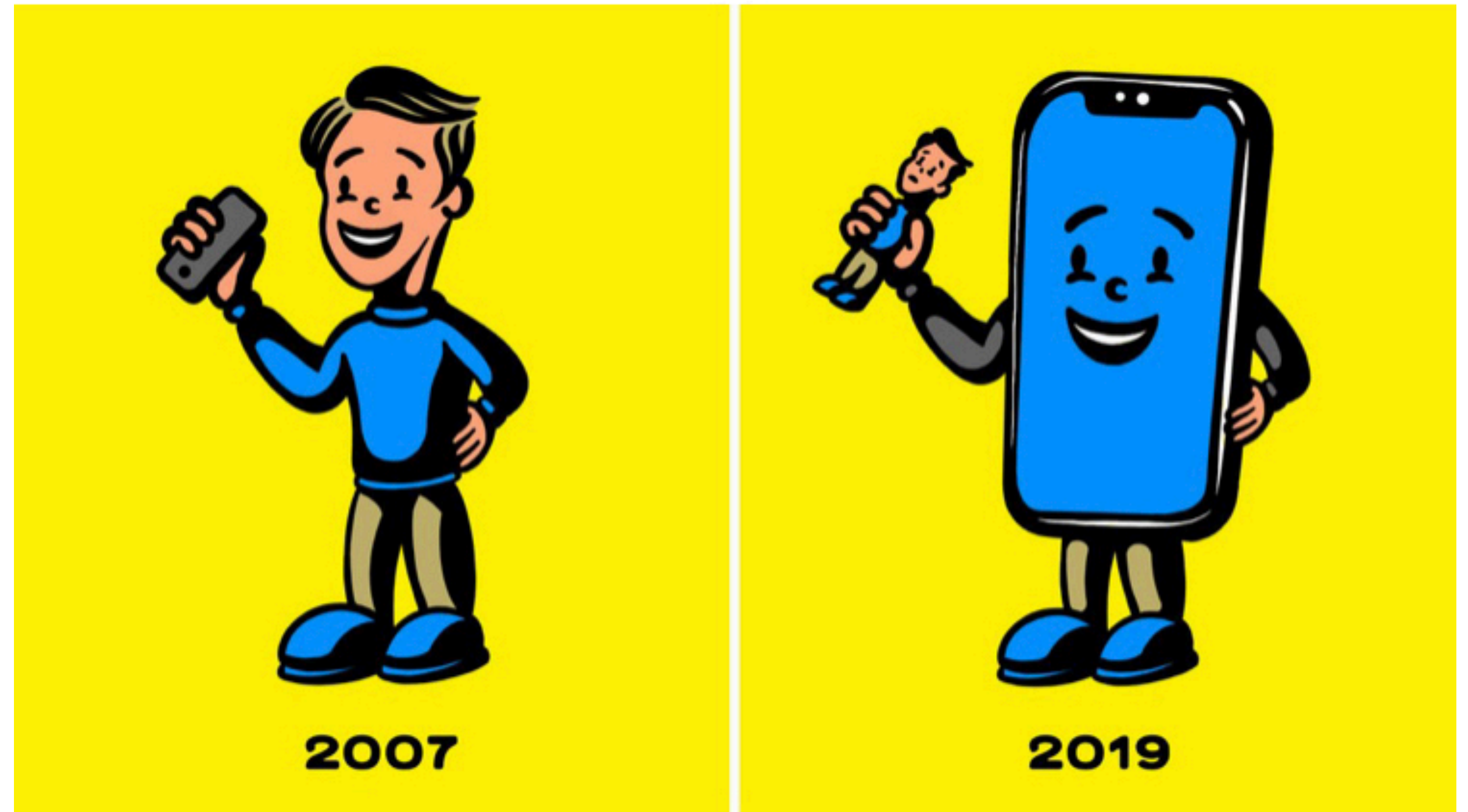
[nlouie.com](http://nlouie.com) Rev20210420





# Topics Covered

- In the news (April 2021)
- Malware, Ransomware 🦠
- Phishing 🐟
- Web Privacy, Cookies 🍪, and Tracking Scripts 🔦
- What makes a *good/bad password*?  
🔑 Using multi-factor auth

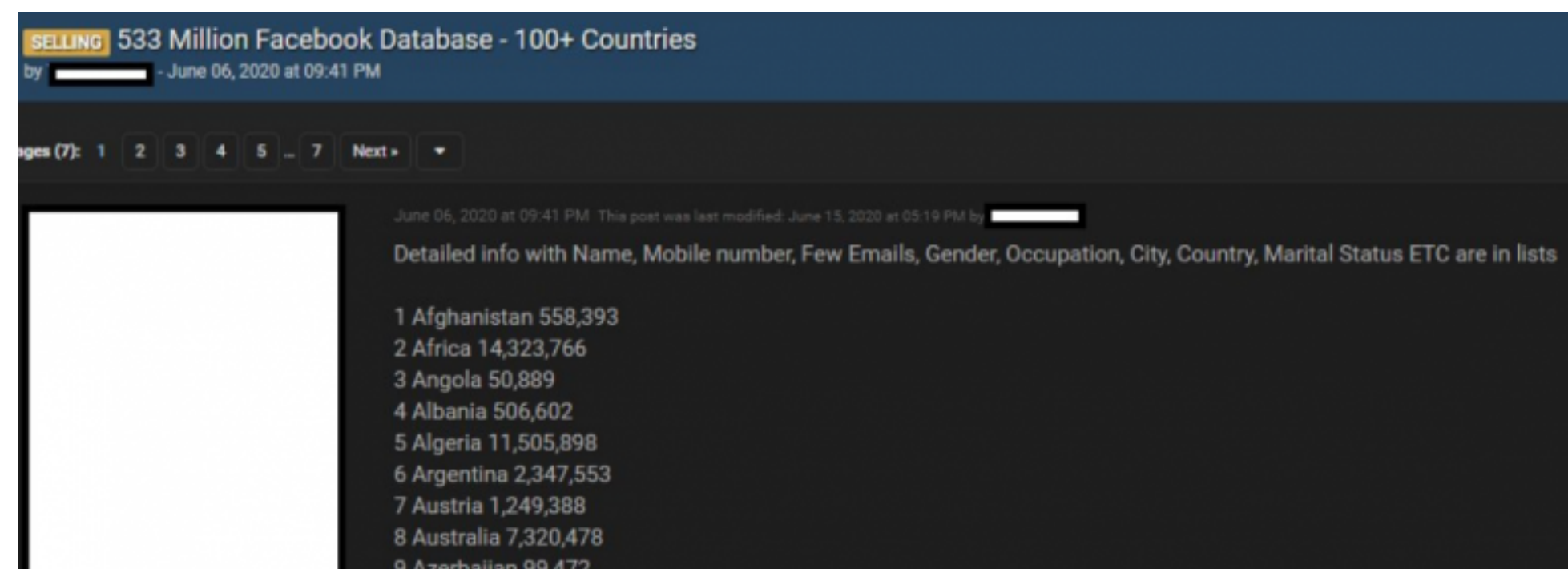




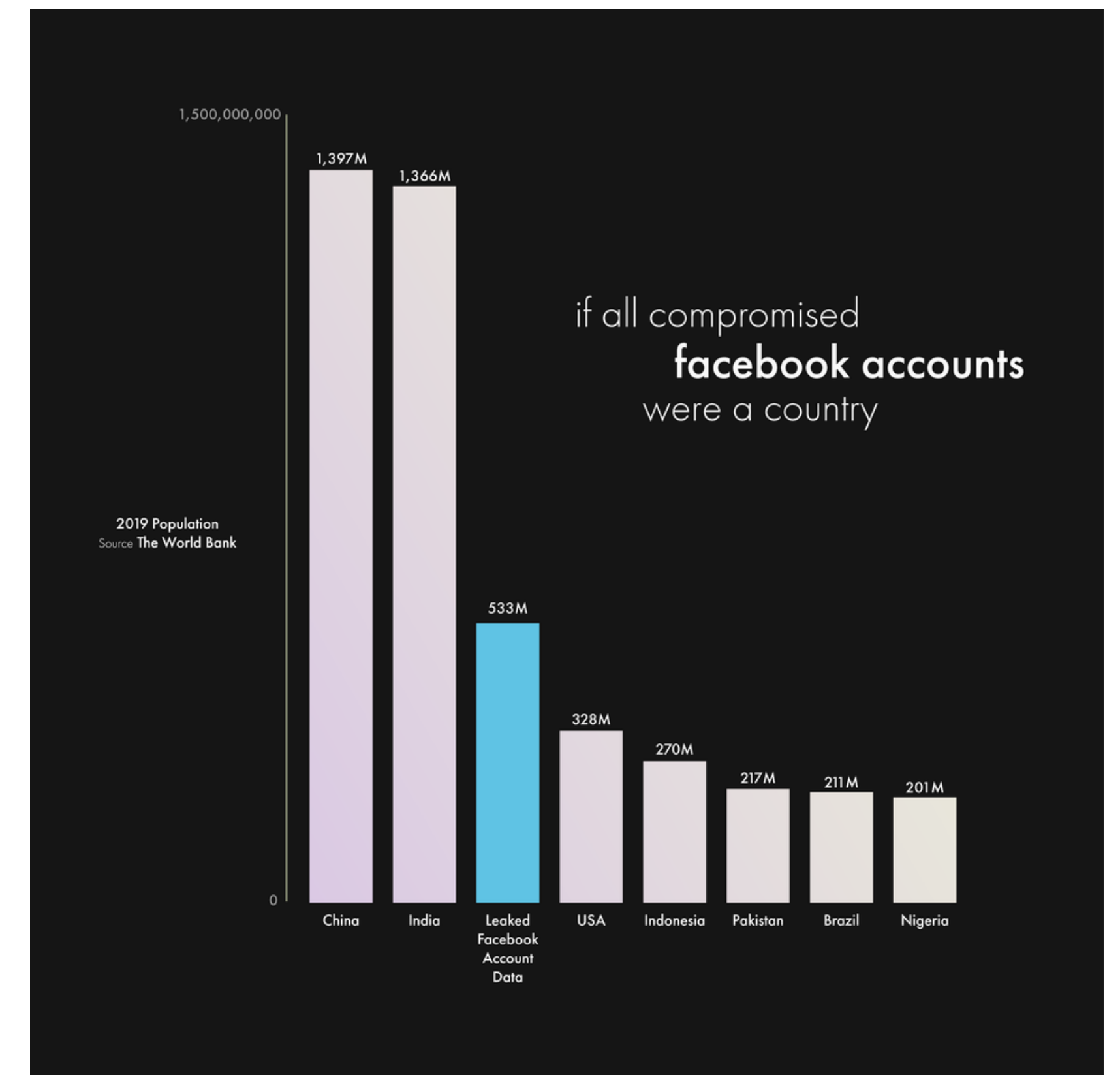
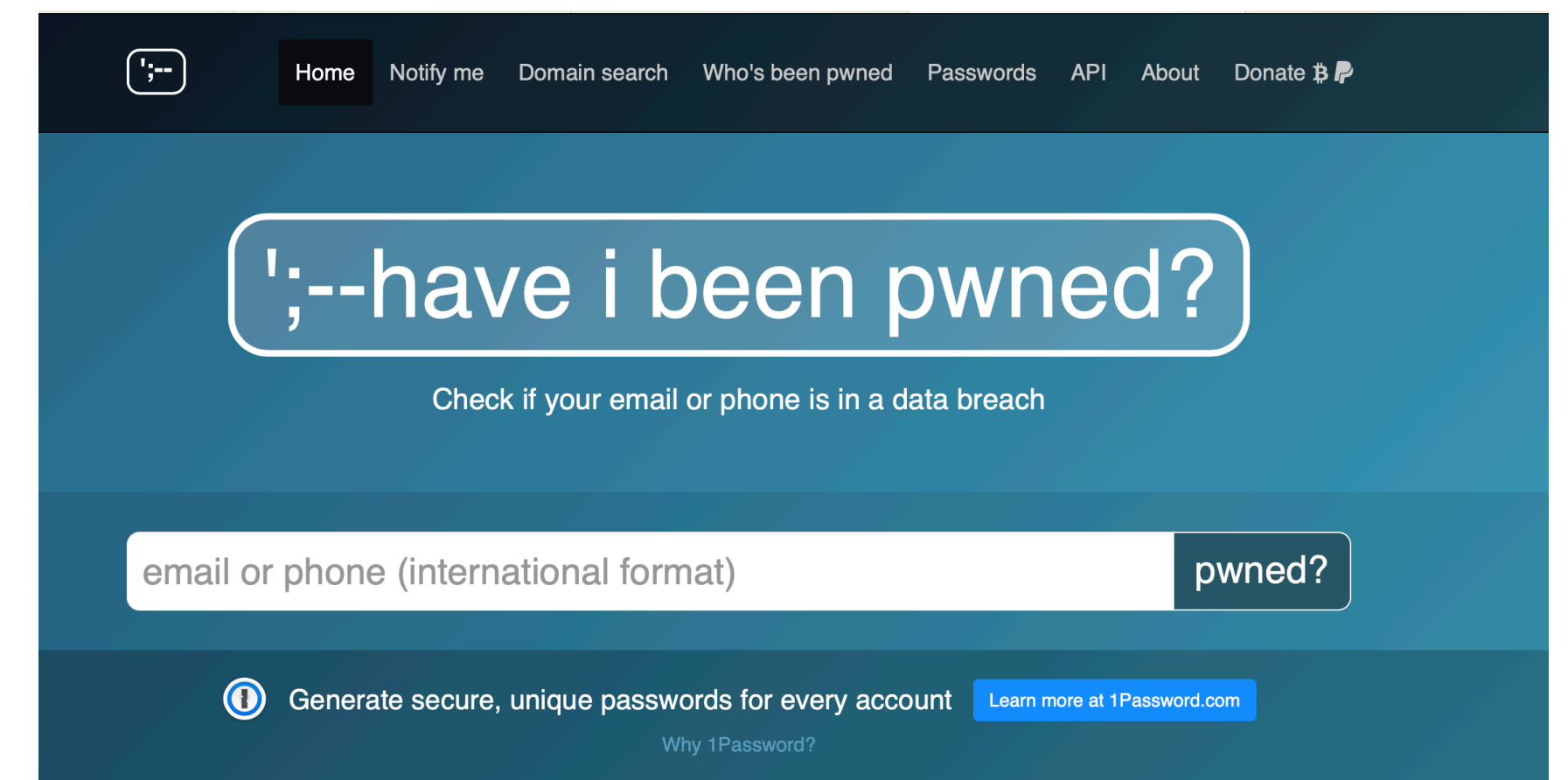
# In the News (April 6, 2021)

## “Are You One of the 533M People Who Got Facebooked?”

- “The *533 million* Facebook accounts database was first put up for sale back in June 2020, offering Facebook profile data from 100 countries, including **name, mobile number, gender, occupation, city, country, and marital status.**”
- You can check if you email or phone number is affected at <https://haveibeenpwned.com>



<https://krebsonsecurity.com> , <https://security.stackexchange.com>



# In the News (March 2, 2021)

**“At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft’s Email Software”**

- At least **30,000 organizations** across the United States (**small businesses, towns, cities and local governments**) were hacked by a Chinese (PRC) cyber espionage unit that’s focused on stealing email from victim organizations, multiple sources tell KrebsOnSecurity. The espionage group is exploiting four newly-discovered flaws in Microsoft Exchange Server email software, and has seeded hundreds of thousands of victim organizations worldwide with tools that give the attackers total, remote control over affected systems.”

<https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software>

<https://www.schneier.com/blog/archives/2021/04/nsa-discloses-vulnerabilities-in-microsoft-exchange.html>

# In the News

## What does it mean?

- Data leaks, breaches, exposures, and exploits happening to individuals, companies, and governments are nothing new. If anything, we are becoming fatigued of cybersecurity news.
- Our lives are becoming more connected, creating more opportunities for exposure, and increasing the risk of personal harm to individuals and groups.
  - How long could you survive without electricity?
    - How long could the *entire East Coast* survive without electricity? <https://www.nbcnews.com/news/us-news/departments-energy-says-it-was-hacked-suspected-russian-campaign-n1251630>
  - Often times it's the most vulnerable that are affected the greatest
    - Political leaders, political opposition, activists, journalists, protestors, rural inhabitants, professionals. [Al Jazeera journalists 'hacked via NSO Group spyware'](#)
- Data hygiene practices requires training, and due diligence.



# Malware

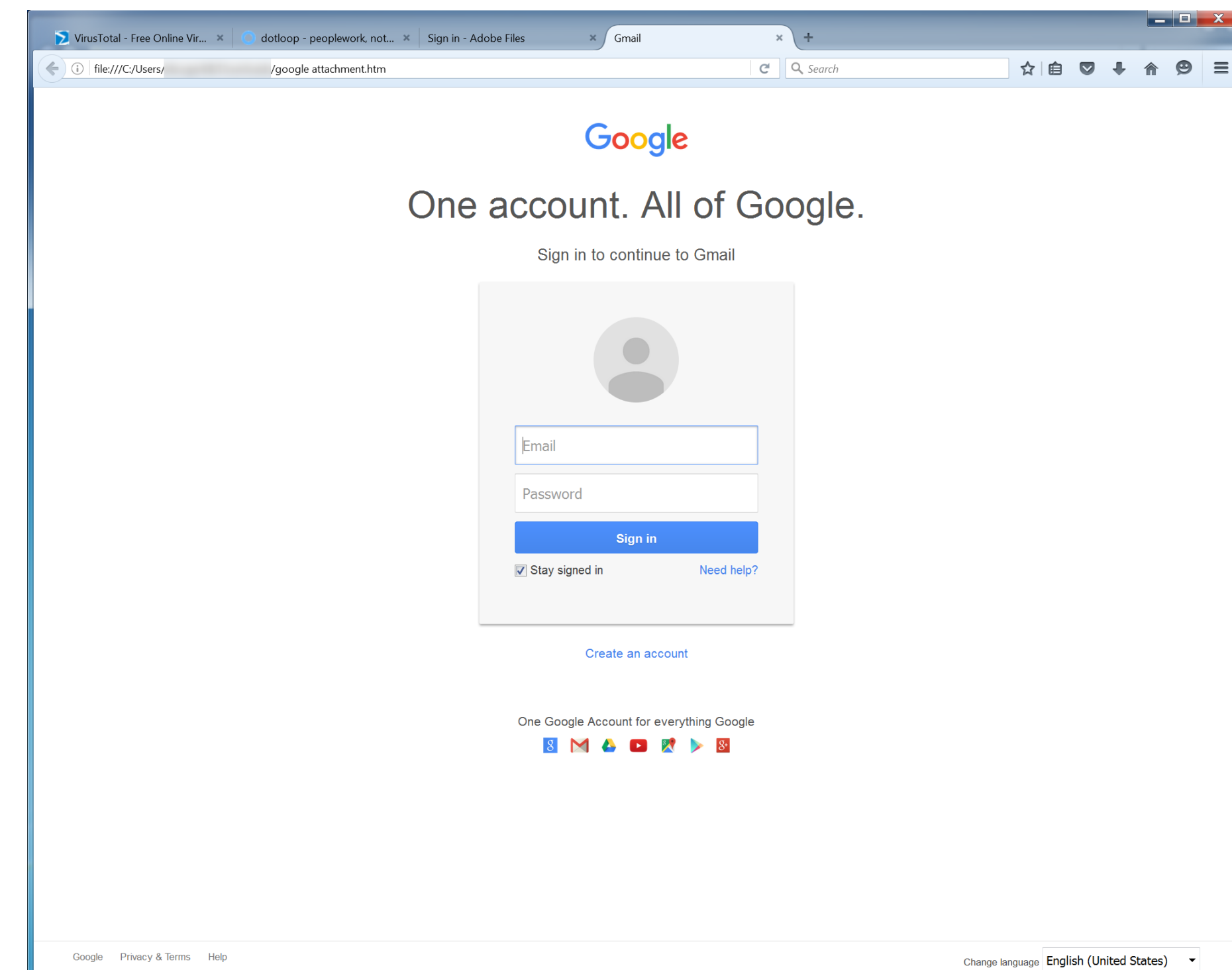
Malware is any **software** intentionally designed to cause damage to a **computer, server, client, or computer network**. Includes **computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper and scareware**.

- Years ago the story went like this...you illegally download some free music online...it requires installing something...eh...why not?
  - Congrats, you got some free ads!! Grow your business by 10 inches!!
- Today...Viruses are not so docile.
  - Computers are hijacked as zombies to be used by crime rings, waiting until they are activated remotely. (Botnets) <https://www.bitdefender.com/box/blog/iot-news/iot-botnet-attacks-rise-2020/>
  - Ransomware encrypts your files
    - “You must send us 1 BTC (today ~\$56,000) within 5 days to recover your files.  
<https://www.cnn.com/2020/10/28/politics/hospitals-targeted-ransomware-attacks/index.html>

# Phishing

## Another reason to dislike phish pics

- **“Phishing emails and text messages may look like they’re from a company you know or trust.** They may look like they’re from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.”
- By impersonating a service with a similar-looking website, the attackers try to steal your login information, and other personal info.

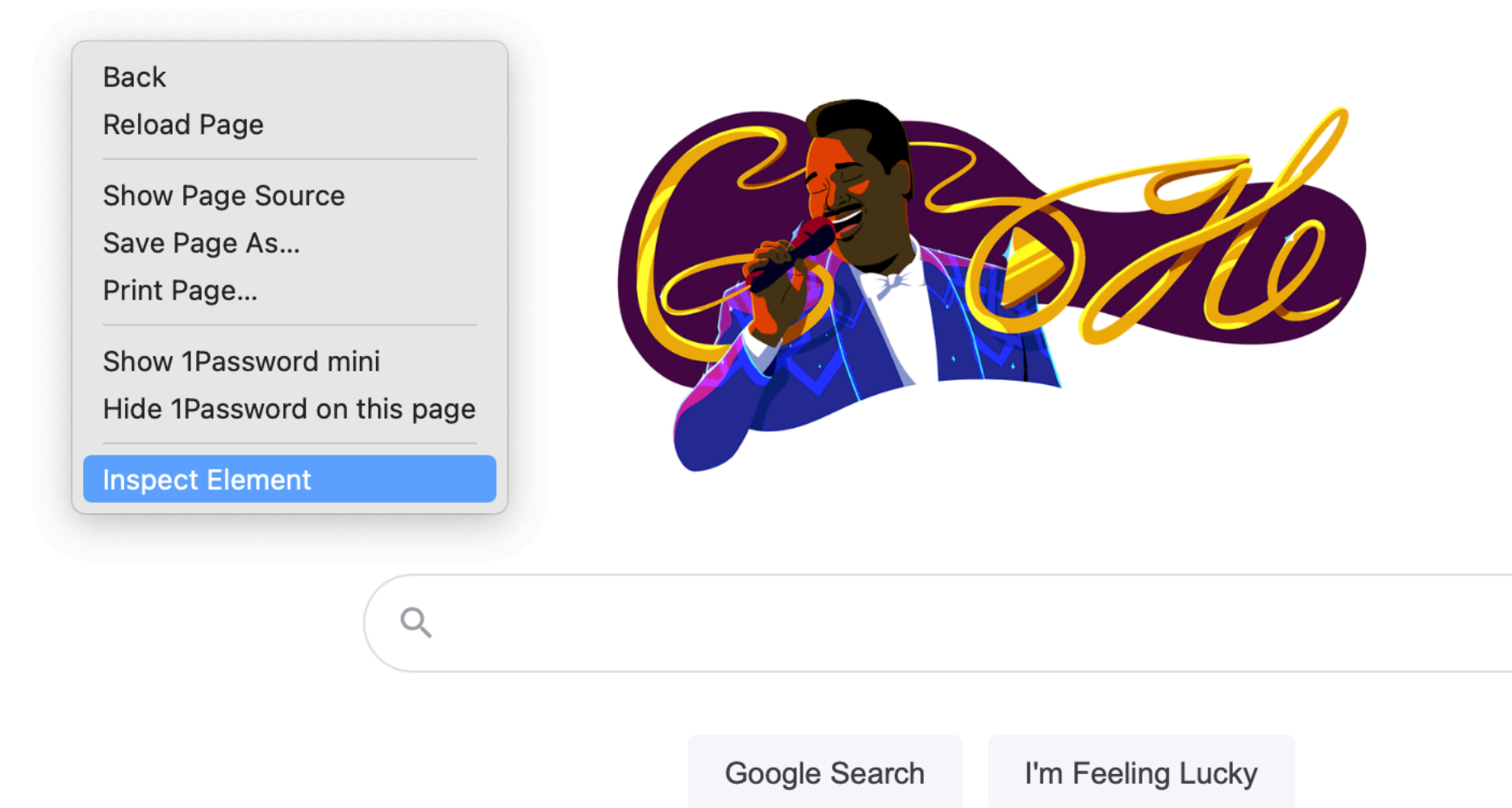


<https://en.wikipedia.org/wiki/Phishing>

<https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

# Web Privacy, Cookies, Tracking Scripts

- Your web browser can leak a lot of data about you
- A cookie 🍪 is some data saved by a website on your browser.
  - operating system, IP address, screen size, geo-location, accelerometer
  - Used to stay logged in, generate better suggestions, analyze marketing behavior.
  - Also used to track users across websites
    - Tracking your web history allows advertisers to send you more relevant ads.



- Check how much data your browser leaks
  - <https://browserleaks.com>
  - <https://coveryourtracks.eff.org>

The screenshot shows the Chrome DevTools Storage panel. The left sidebar lists storage types: All Storage (selected), Application Cache, Cookies (selected), Local Storage, and Session Storage, all for the domain www.google.com. The main panel displays the Cookies table with the following data:

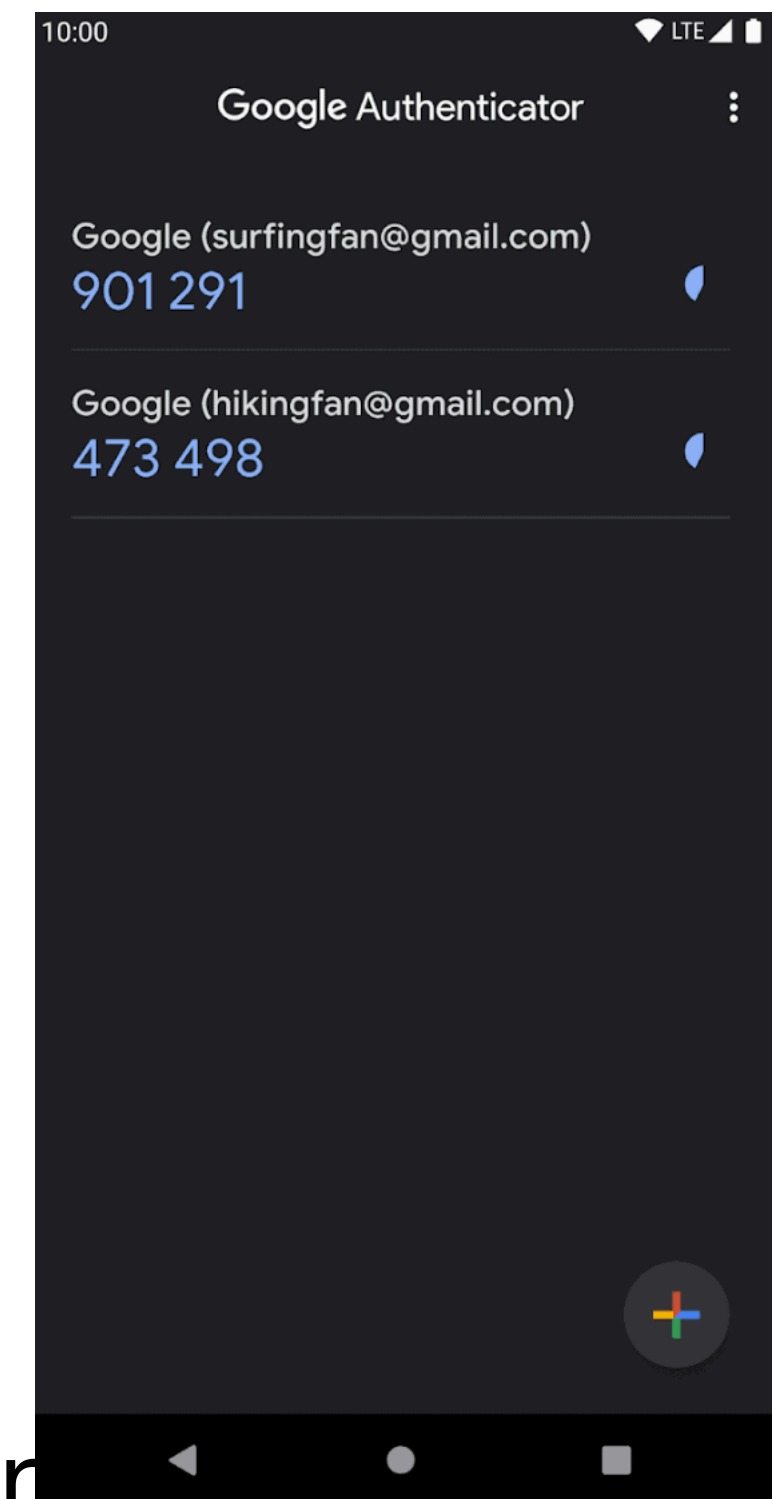
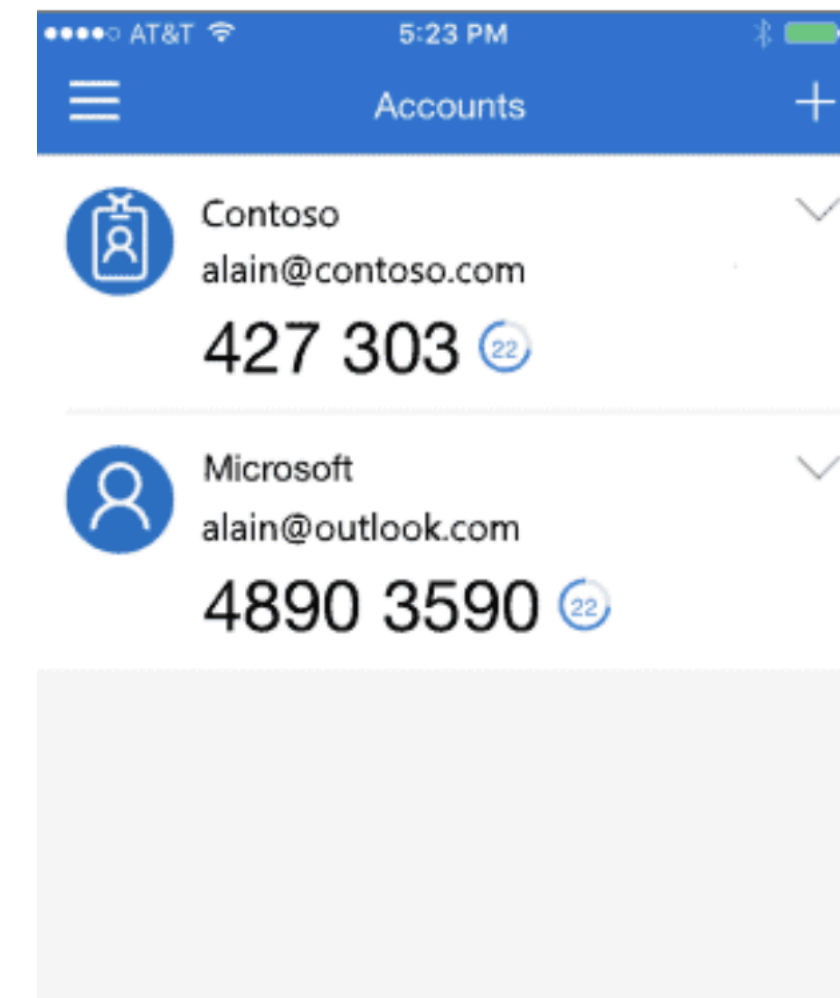
Name	Value	Domain	Path	Expires	Size	Secure	HttpOnly	Same...
1P_JAR	2021-04-21-01	.google.com	/	5/20/2021, 9:55:...	19 B	✓		—
NID	214=sVffLAnEWxIPtnsZcyXZAc...	.google.com	/	10/20/2021, 9:55:...	178 B	✓	✓	—



# Passwords

## What makes a good password?

- Never reuse passwords.
- Forget password rules, or l33tP4ssw0rds.  
Use a password manager to generate passwords instead
  - Check if your password has been part of a data breach <https://haveibeenpwned.com/Passwords>
- Use multi-factor authentication (2FA/MFA). If your password is stolen, then the second key (on your phone) still prevents anyone from logging in.
  - Phone number verification is still vulnerable to SIM Swapping, where an attacker takes over your phone #, usually through social engineering
  - Preferably, use a physical key, like a Yubikey



# What can I do?

## 10 Things You Would Never Believe To Do To Defend Yourself From Cyber Attacks

- Only give out the minimum information necessary to access a system. Does this website *really* need your birthday?
- Use a password manager.
- Keep your devices updated! Updates often include critical security patches.
- Use a privacy respecting browser, like Firefox, or Brave .. or at least Safari on Mac.
- Install privacy browser extensions, and remove disreputable ones.
- Use a VPN, or host your own
- Never click links in suspicious emails, text messages, or give away personal data to someone over the phone. If it sounds too good to be true, it probably is.