Privacy Champions

Privacy Tips for Email & Social Media

June 26, 2019

Agenda

Email

Social Media

Privacy Tips

Email

Email has many benefits, but also presents risks

Email has become secondhand and oftentimes people can respond to an email without knowing the risks.

In addition to the privacy concerns involved with emailing sensitive information, security risks also exist, particularly due to **social engineering** and **phishing** attacks.

Phishing is currently one of the County's most prolific attack vectors.

Government and Business leaders alike have learned this lesson the hard way (e.g., 2016 Democratic campaign revelations, Financial firm wires $5 million).

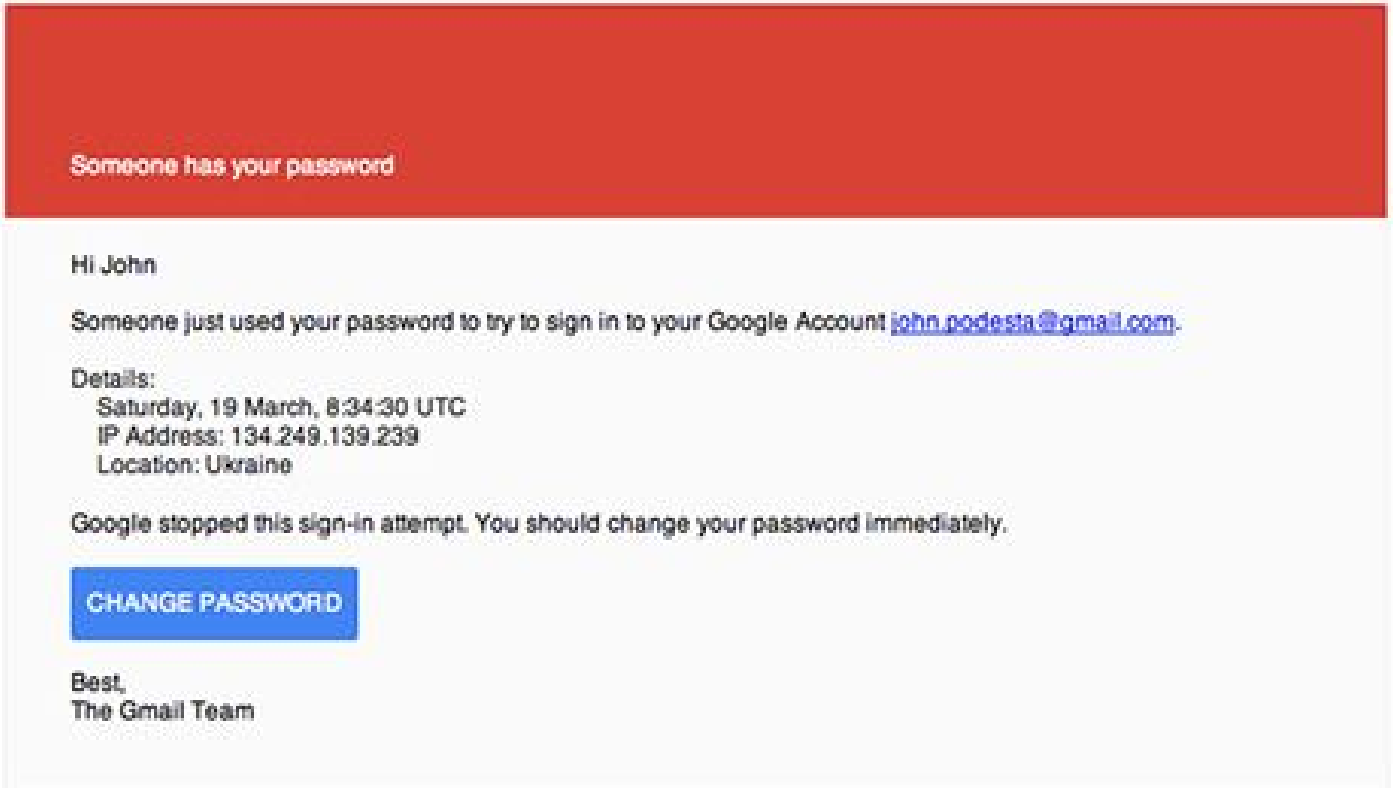
The County Privacy Office works with the Information Security Office, and we can discuss approaches you may take so that this doesn't happen to you (or a member of your team).

Details from Robert Mueller's July 2018 Russia indictment provide examples of how social engineering and phishing work in practice

- Russians targeted over 300 people affiliated with the 2016 Clinton Campaign, the Democratic Congressional Campaign Committee (DCCC), and the Democratic National Committee (DNC).

- Through social engineering, the Russians, who worked for a military intelligence agency called the Main Intelligence Directorate of the General Staff (GRU), successfully gained access to several Clinton Campaign, DCCC, and DNC accounts, including the account of John Podesta, the chairman of the Clinton Campaign as well as Debbie Wasserman Schultz, the DNC chair.

Mueller indictment: Email sent to John Podesta, Senator Clinton's campaign chair



Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

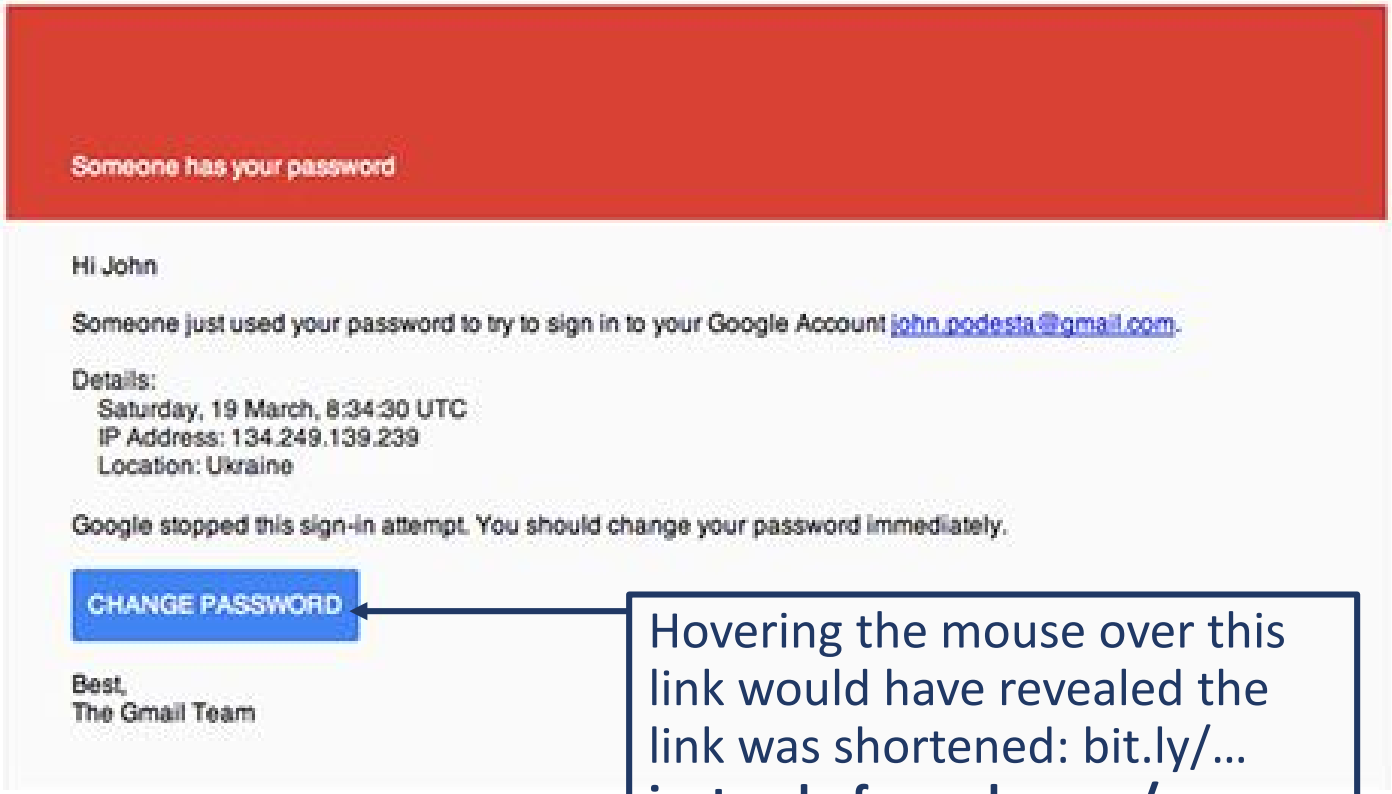
Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

Source: The Smoking Gun

Email elements: Check links



Hovering the mouse over this link would have revealed the link was shortened: bit.ly/…
instead of google.com/…

Mueller Indictment: Google password reset email to John Podesta, Clinton Campaign chairman

- The GRU sent an email to the chairman of the campaign. They **altered the sender's email address in order to make it look like the email was a security notification from Google** (a technique known as **"spoofing"**). The sender address looked legitimate: no-reply@accounts.googlemail.com.

- The email **instructed the chairman to change his password** by clicking an embedded link. The link directed to a GRU-created website that looked like a legitimate Google webpage to change a password.

- When the chairman's login information was entered into the GRU-created website, the Russians gained access to the login information and thus to **the contents** of the chairman's email account, which contained **over 50,000 emails**.

- Many of these emails were then **leaked to the public** through online personas such as "DCLeaks" and "Guccifer 2.0." These online personas were used to hide the fact that Russia, a state actor, was behind the phishing campaign.

- Although the chairman's emails were relatively scandal free, they diverted attention and provided extreme detail into the campaign's strategy.

Mueller Indictment: “spearphishing” emails sent to campaign staffers

- In another attempt to gain access to Clinton Campaign information, the GRU used an email account with a **one-letter deviation** from a known member of the Clinton Campaign to email over thirty different employees. For example:
  - REAL: john@ceo.sccgov.org
  - FAKE: john@ceo.scegov.org

- The email contained an embedded link to a Microsoft Excel file titled “**Hillary-clinton-favorable-rating.xlsx**.” The senders knew that the title of this link would be enticing to the recipients.

- In fact, the Excel link directed users to a GRU-created website. This was a fake website that prompted targets for their login credentials.

Mueller Indictment: access to Clinton Campaign and DCCC leads to access to the DNC

- Armed with the **login credentials** of a DCCC contractor authorized to gain access to the DNC network, the GRU infiltrated the national committee, eventually gaining access to 33 computers.
- Once inside DCCC and DNC computers, hackers searched for keywords related to the 2016 election.
- In mid-April 2016, they searched one DCCC computer for terms including: “hillary,” “cruz” and “trump.”
- The hackers also copied particular DCCC folders, including one labeled “Benghazi Investigations.”
- They also targeted computers that contained information about opposition research and “field operation plans” for the 2016 election.
- The emails and documents were then released over time through DCLeaks and Wikileaks.
- **Consequences**:
  - Hillary Clinton, Presidential Candidate – The breached data and emails along with the exposure of the breach may have led, in part, to election loss
  - Debbie Wasserman Schultz, DNC Chair – Resigned
  - Amy Dacey, DNC CEO – Resigned
  - Brad Marshall, DNC CFO – Resigned
  - Luis Miranda, Communications Director – Resigned
  - Democratic Party – Damaged by revelations about intra-party conflict between the Hillary Clinton and Bernie Sanders campaigns

Other examples of government phishing attacks

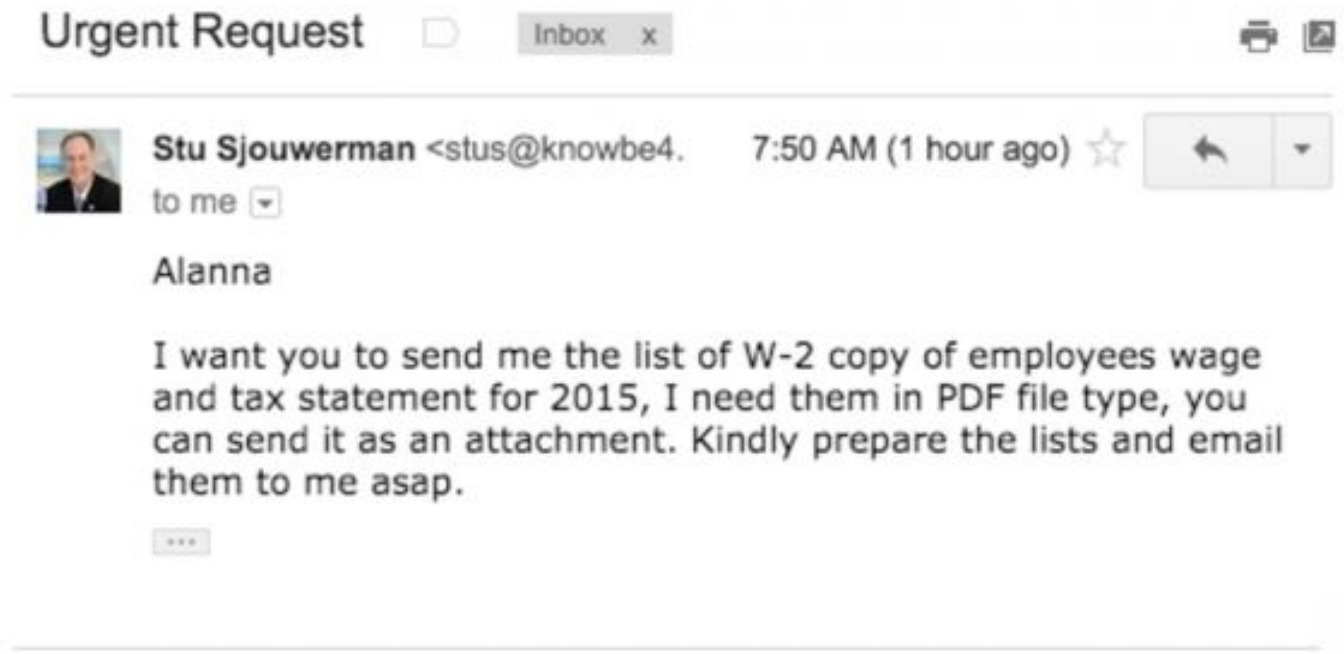
"Scammers will do their homework about a town's front office, going so far as to read emails from a mayor and imitating writing style."

Mike Hamilton, former Seattle CIO

- August 2018, Hennepin County, Minnesota
  - Using e-mails disguised as pay-raise notifications, a sophisticated phishing scam duped the employees into giving up their login information, then used their official e-mail accounts and signatures to spread the attack to other contacts, according to county officials.

- August 2017, Yarrow Point, Washington
  - Emails disguised as being from the town mayor were sent to the town's fiscal coordinator requesting wire transfers. This eventually led to the loss of ~$50,000.

Example: Phishing for Personal & Financial Information



https://krebsonsecurity.com/2016/02/phishers-spoof-ceo-request-w2-forms/

Social Engineering Attack Profile

- Social Engineers may research people the same way criminals conduct pre-planning. They may research you or your organization to build rapport as part of their scheme:
  - Learn about your beliefs (e.g., religious, political, social)
  - Learn about your place of work, your job, postings you have made about personal or work-related issues
- Cyber criminals can “spoof” or imitate phone numbers and email addresses:
  - Caller ID can be spoofed to display a 1-800 number or use your home area code to add authenticity
  - They create a sense of urgency so that you don’t have time to think
- They may use existing knowledge to provide validity to the call or email:
  - Use directories to find your home address, place of employment, date of birth, phone number, email address, etc.
  - May use information from a previous data breach
  - And they may use this information to try and build trust

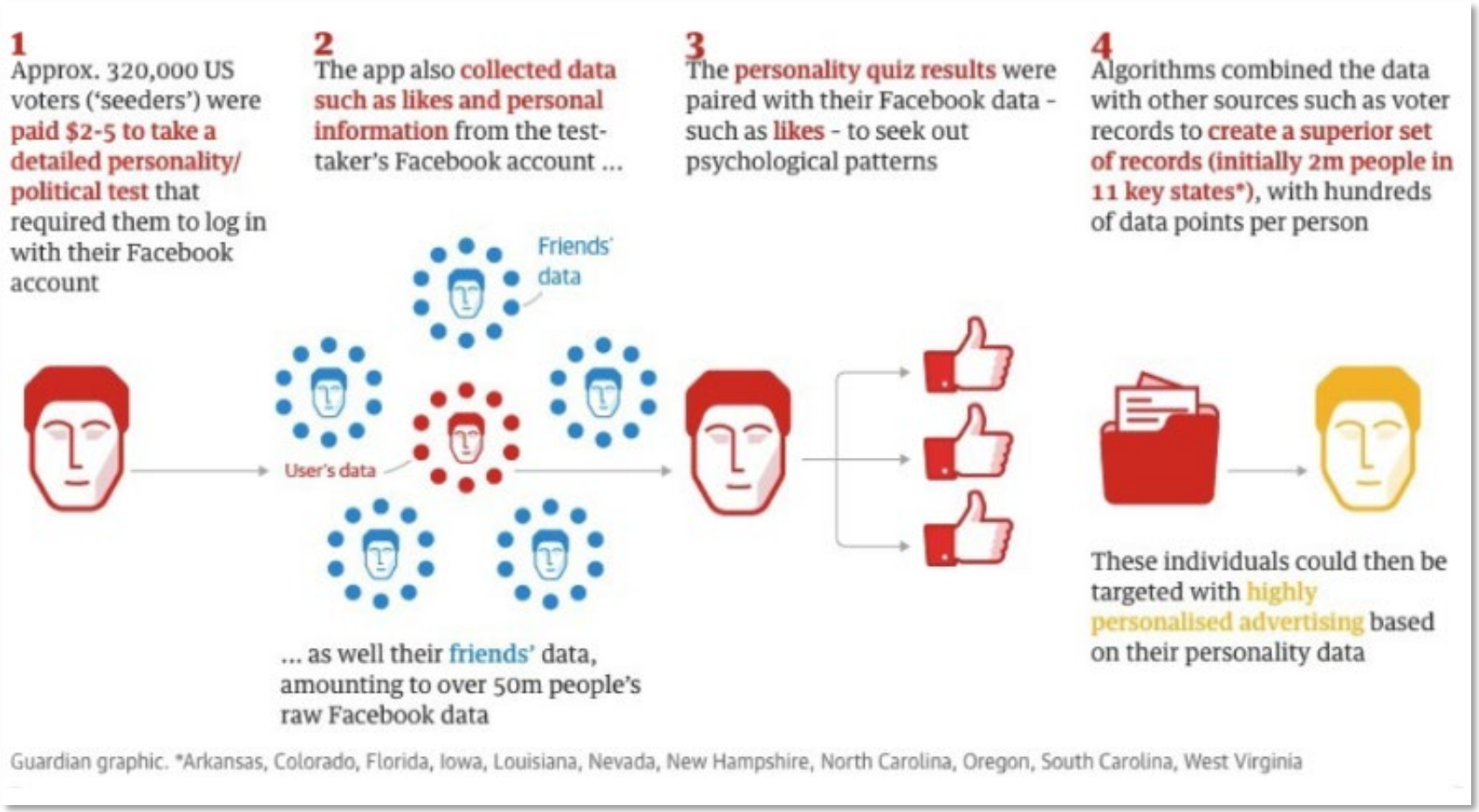
Social Media

What is Cambridge Analytica and how can they impact political campaigns and government?

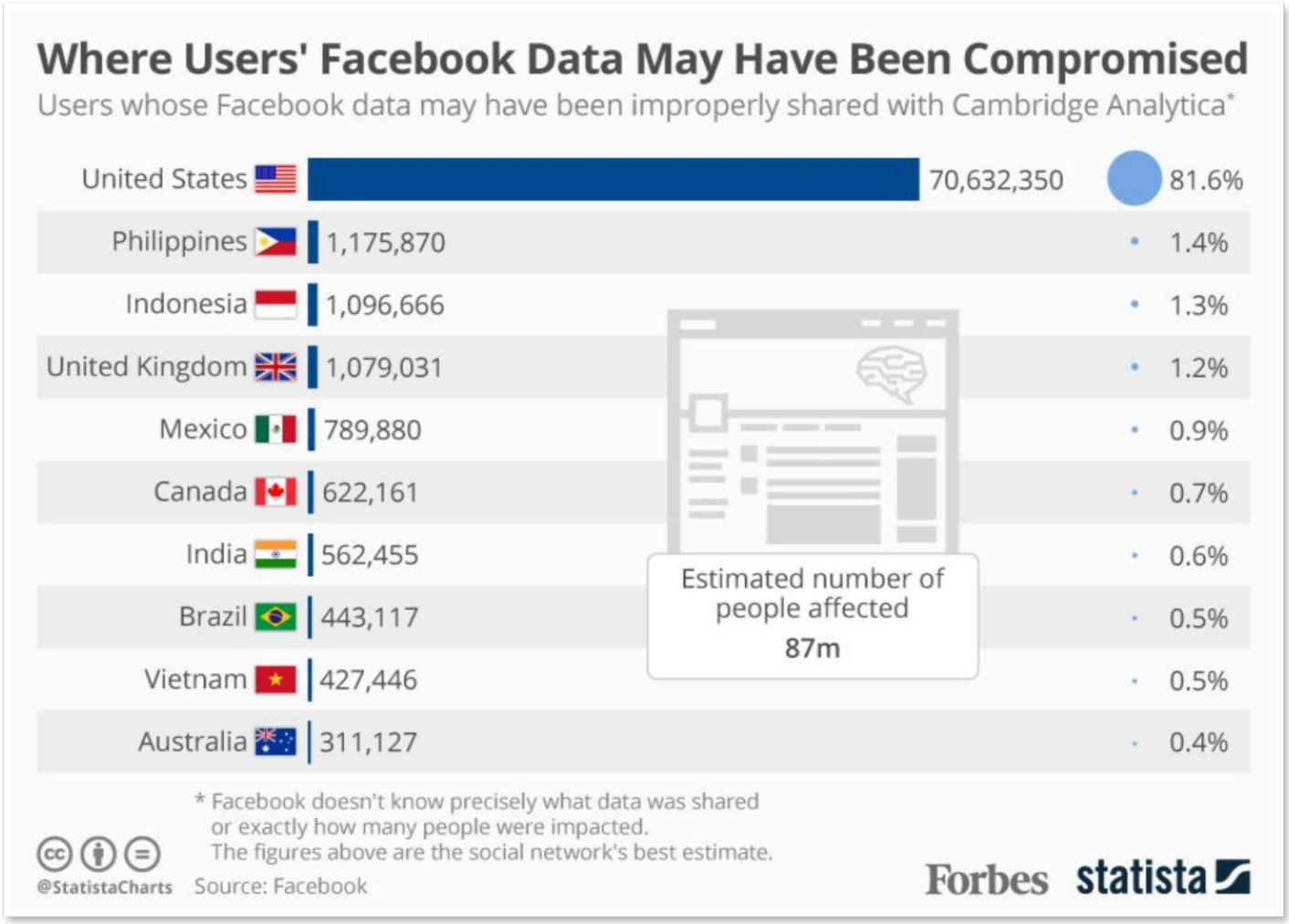
- Prior to the Facebook / Cambridge Analytica incident, many people had never heard of the company or understood its model in data mining and analysis.
- Not surprisingly, users also did not know that their information could be shared with/resold to third parties without their knowledge or consent.
- Cambridge Analytica's political arm worked with government entities, political action committees, and private interests to provide its service offerings.

How did it happen? Cambridge Analytica's data mining methods come into question

Cambridge Analytica was able to acquire over 70 million of U.S. Facebook records, many without user consent, and did not directly violate any laws. How did it happen?

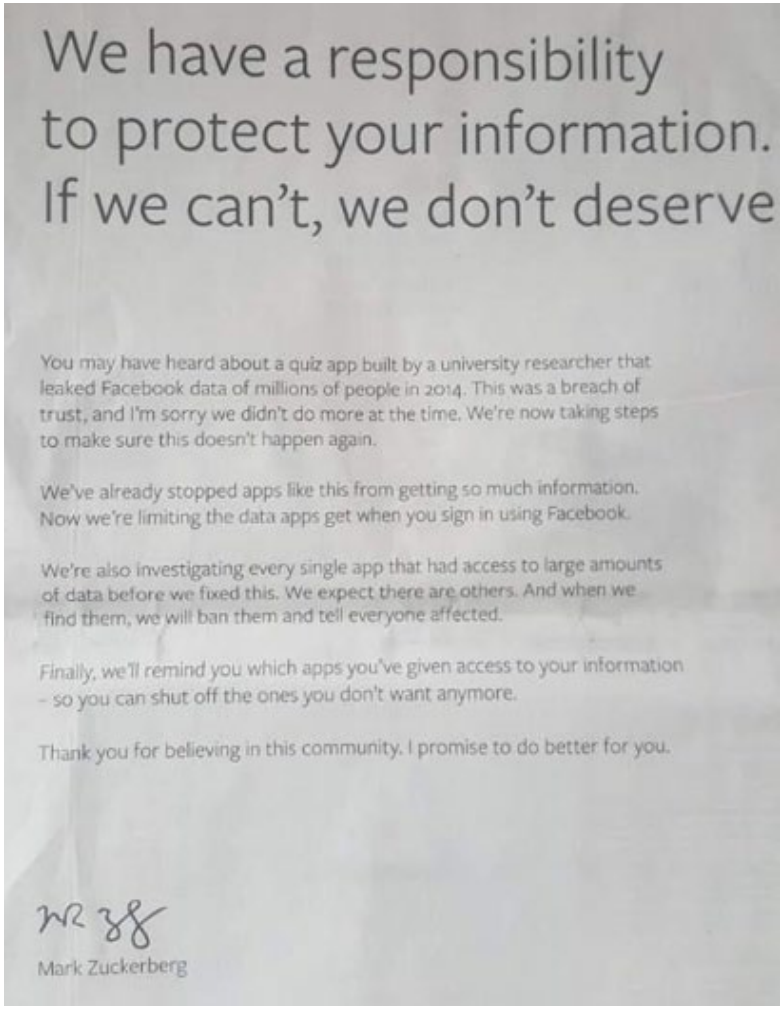


While the Facebook / Cambridge Analytica incident primarily impacted the U.S., international users also fell prey



Proactive organizations think of privacy upfront as an enabler not a deterrent to effective operations

- Organizations often think of privacy as an extra step or expense, and they typically react to crisis events during and after they occur when most of the damage has already been done
- The highest levels of leadership are starting to feel the impact of neglecting privacy
- *Lesson Learned*: Proactively manage privacy, social media practices, and user behavior expectations upfront or pay the price later



We have a responsibility to protect your information. If we can't, we don't deserve

You may have heard about a quiz app built by a university researcher that leaked Facebook data of millions of people in 2014. This was a breach of trust, and I'm sorry we didn't do more at the time. We're now taking steps to make sure this doesn't happen again.

We've already stopped apps like this from getting so much information. Now we're limiting the data apps get when you sign in using Facebook.

We're also investigating every single app that had access to large amounts of data before we fixed this. We expect there are others. And when we find them, we will ban them and tell everyone affected.

Finally, we'll remind you which apps you've given access to your information – so you can shut off the ones you don't want anymore.

Thank you for believing in this community. I promise to do better for you.

Mark Zuckerberg

Response to Facebook and Cambridge Analytica incident, Mark Zuckerberg, CEO, Facebook, 2018

Social media “bots” have changed the way government and commercial enterprises interact with the public

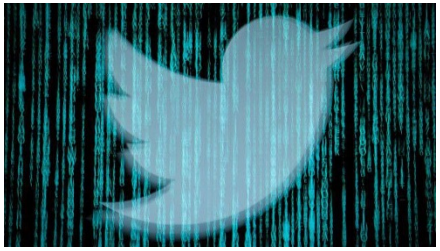
- What is a “bot” in social media?
  - A bot is a software application that can mimic common user responses on social media platforms, such as Twitter, to include: likes, retweets, and even content generation (e.g., messages, replies, etc.)
  - Bots may be used to generate interest, bolster a cause, or damage reputations
  - Adding likes and retweets may add credibility to an article or a cause and may artificially manipulate search engine optimization (e.g., bumps up the priority creating a falsely popular article or moves up a link in Google search results)
  - A simple bot application could create a few accounts or millions
  - Each set of bots can be programmed to follow a certain agenda or target real individuals who fit a certain profile, such as those who may be more susceptible to targeted content

The actual and reputational risks bots pose to an organization's legitimate operations may be extensive

- What are the risks that organizations need to know:
  - Sometimes generated interest may be for a positive cause
    - Increase visibility and elevate search result placement for a food drive
    - Create buzz for a rally to increase teacher pay
  - Politically, generated interest can be used to spread and add credibility to bogus news articles, false or misleading information, and fake responses to actual users
  - Government agencies and companies, large and small, may be subject to a targeted campaign from:
    - Political interests
    - Foreign adversaries
    - Corporate competitors
    - Hacktivists who attempt to spread negative press for a personal cause
  - Consumers and constituents may believe in the false content perpetuated by bot accounts and may retweet, like, and show support for causes that damage the credibility and reputation of government and businesses

“Bot” accounts attempt to mimic the behavior of an actual user and are not immediately recognizable

- Most social media platforms do not require bot accounts to identify themselves easily
- People can be fooled into believing they are interacting with or relying on the knowledge of an actual person, when they are potentially being misled or manipulated by a bot
- A few telltale signs can help users reveal a bot account:
  1. They are telling you they are a bot (Sometimes they are obvious)
  2. Getting a direct response on your tweet, especially from a user you do not know
  3. Huge amount of accounts following, small amount of followers
  4. They tweet the same thing to everybody
  5. The follow / unfollow game
  6. Duplicate profile pictures
  7. Coming from an API



PRIVACY TIPS

Email Tips: Identify and avoid threats

- Use alternative and known methods of communication
  - Call the Manager, Co-worker, Bank, etc. directly from a directory
  - Visit the webpage directly by typing in the domain yourself
  - Avoid providing any personal or sensitive information via email or cold call
- Phishing will only continue to get more sophisticated and difficult to decipher
  - Don’t assume you can tell the difference, even security professionals can be fooled
- Data loss prevention (DLP) tools can help identify spam and prevent sensitive information from leaving secured environments

Email address auto-complete is easier and usually gets it right, so why should I bother checking it?

A staff member wants to send a colleague a file containing sensitive information in an email attachment. As s/he types the email address, Outlook automatically populates it and s/he sends it, but it goes to the wrong person.

Risk	Recommendation
There is always a risk of an unintended disclosure when an email is sent to the wrong person. The auto-complete feature (e.g., when Outlook automatically fills in an email address after you type in a few letters of a person's name) is popular and standard in many email applications. While it offers convenience, it is possible that auto-complete inserts the wrong email address and may lead to sensitive information going to the wrong person.	Always double-check the recipient when sending emails, especially when using auto-complete. They should always encrypt emails and encrypt or password-protect any attachments that contain sensitive information. Any accidental disclosures or mistaken emails should be reported immediately.

Email & Social Media Accounts: Protect your data

- Protect Your Personal Information
  - Lock down your login: Protect your online accounts by enabling multifactor authentication.
  - Change your password on a regular basis and make your password a sentence (passphrase): Make your password long, strong, and complex.
  - Unique account, unique password: At a minimum, separate your work and personal accounts and make sure that your critical accounts have the strongest passwords and are not duplicated.
  - Keep it safe: Everyone can forget a password. You can alternatively use a service like a password manager to keep track of your passwords.

Social Media Tips: If my data is already out there, why do I need to manage my privacy and security settings?

Doing nothing is the same as leaving your door wide open

- It may seem like a lost cause to continue to be vigilant in protecting your data
- For those who do, it seems like an uphill and changing battle when companies alter their privacy policies and settings, sometimes with little notice and confusing details
- Taking a few steps to set privacy and security settings for your organization and yourself can help prevent or deter would-be hackers
- For instance, in the Facebook / Cambridge Analytica incident, those users whose privacy settings did not allow third-party data sharing were not exposed or targeted
- Take a moment to review updated privacy policies or at least check your accounts from time-to-time to make sure you stay aware of the way your information is handled

PRIVACY OFFICE

COUNTY OF SANTA CLARA

Email: PrivacyOffice@ceo.sccgov.org

Internal website: https://sccconnect.sharepoint.com/sites/cpo

External website for constituents: https://www.sccgov.org/sites/cpo