



digital defense fund

# Data Stewardship & Security

Last updated 3/5/21

# Take a moment to think about what data you store.

What data do you collect & store from:

- Donors
- Employees
- Clients
- Collaborators

What's in your Google Drive/OneDrive? What's in your Slack? What's in your database?



# Threat modeling: How does data get exposed?



Threat modeling  
helps us ground  
our fears in reality



# What is likely?

INCIDENT TYPE	COUNT OF INCIDENTS	COUNT OF SAMPLE	% OF SAMPLE EXPERIENCE INCIDENT
1. Email Phishing	140	41	26%
2. Malware	54	39	25%
3. Account Compromise	20	18	12%
4. Business Email Compromise	14	13	8%
5. Wire fraud	3	3	2%
6. Virus	1	1	1%
7. Advanced Persistent Threat	1	1	1%
8. Supply Chain	0	0	0%
9. Ransomware	0	0	0%
Grand Total	233	116	50%

^^ From Community IT's 2018 Non-profit Cybersecurity Incidents Report

<https://www.communityit.com/wp-content/uploads/2019/03/NonprofitCybersecurityIncidentReport.pdf>



# How does data get exposed?

- Credential theft (someone gets our login)
  - Phishing email
  - Impersonation
  - Reused credentials
  - Guessed passwords (brute force attack)
- Internal bad actor
- Lost or stolen device
- Third party vendor breach



CONTROL, WE HAVE FLOWN TO THE USA AND BREACHED THE TARGET'S HOUSE.

THEY WROTE ALL THEIR PASSWORDS IN A BOOK LABELED "PASSWORDS"!

THE FOOL!



HOW PEOPLE THINK HACKING WORKS

HEY LOOK, SOMEONE LEAKED THE EMAILS AND PASSWORDS FROM THE SMASH MOUTH MESSAGE BOARDS.

COOL, LET'S TRY THEM ALL ON VENMO.



HOW IT ACTUALLY WORKS

Source:  
[xkcd.com/2176/](http://xkcd.com/2176/)



# Realistic example: Canva breach

1. A popular free graphic design website, Canva, was recently breached.
2. Usernames and passwords were released.
3. Canva is commonly used by nonprofits. A bad actor notices a nonprofit's domain in one of the emails.
4. They try that username & password on Salesforce, Gmail, and Dropbox.





# Realistic example: Phishing

1. You get an email from Google saying that suspicious activity has been detected on your account. The email instructs you to click a link to change your password to protect your account.
2. The link goes to `google.secureuraccount.com`. It asks you to sign in with your existing login, then asks to change your password.
3. It all looks legit...but `google.secureuraccount.com` is not a real Google website, it's from someone looking to steal your login!



# Realistic example: third party vendor breach

1. Your organization uses StoreYourStuff's cloud storage for a client spreadsheet.
2. "The cloud" is really just a bunch of servers StoreYourStuff rents from Amazon Web Services (AWS).
3. Amazon discovered a security flaw and released a patch. But StoreYourStuff's IT manager was out and the email about the patch got lost in their inbox.
4. A bad actor discovers that StoreYourStuff didn't patch. They're able to exploit the security flaw to access all the info on the servers and post it for sale on a hacker forum.



# The responsibility of protecting data is shared between platforms and users

## What they control:

- Security of our data in transit
- Security of our data storage
- What and how they share our data with other services, or entities

## What we control:

- Our login
- What and how we share with other services
- What and how we share with other users
- Our devices we use to access those platforms

Solutions: How do you keep your  
data (and coalition members)  
safe?

# 1. Protect against account compromise with Strong Credentials & 2FA

# The responsibility of protecting data is shared between platforms and users

## What they control:

- Security of our data in transit
- Security of our data storage
- What and how they share our data with other services, or entities

## What we control:

- **Our login**
- What and how we share with other services
- What and how we share with other users
- Our devices we use to access those platforms



# What makes a strong password?

Let's check some passwords at [howsecureismypassword.net](https://howsecureismypassword.net) to see...



# How Secure Is My Password?

 The #1 Password Strength Tool. Trusted and used by millions.

Your password would be cracked

# Instantly



# How Secure Is My Password?

 The #1 Password Strength Tool. Trusted and used by millions.

hg7Vtzy#



It would take a computer about

**8 hours**

to crack your password

# How Secure Is My Password?

 The #1 Password Strength Tool. Trusted and used by millions.

hg7Vtzy#45fw2s



It would take a computer about

# 2 hundred million years

to crack your password

# How Secure Is My Password?

 The #1 Password Strength Tool. Trusted and used by millions.

 silly brutal safe travel 

It would take a computer about

**3 sextillion years**

to crack your password

If my password is strong, why does it need to be unique?

Remember that comic? Sites get breached all the time, and hackers can access your passwords from breached sites.

Let's [check haveibeenpwned.com](https://haveibeenpwned.com) to see if a hacker already could have your password...



Remembering unique, complex passwords for every account is VERY hard.

That's why password managers exist!

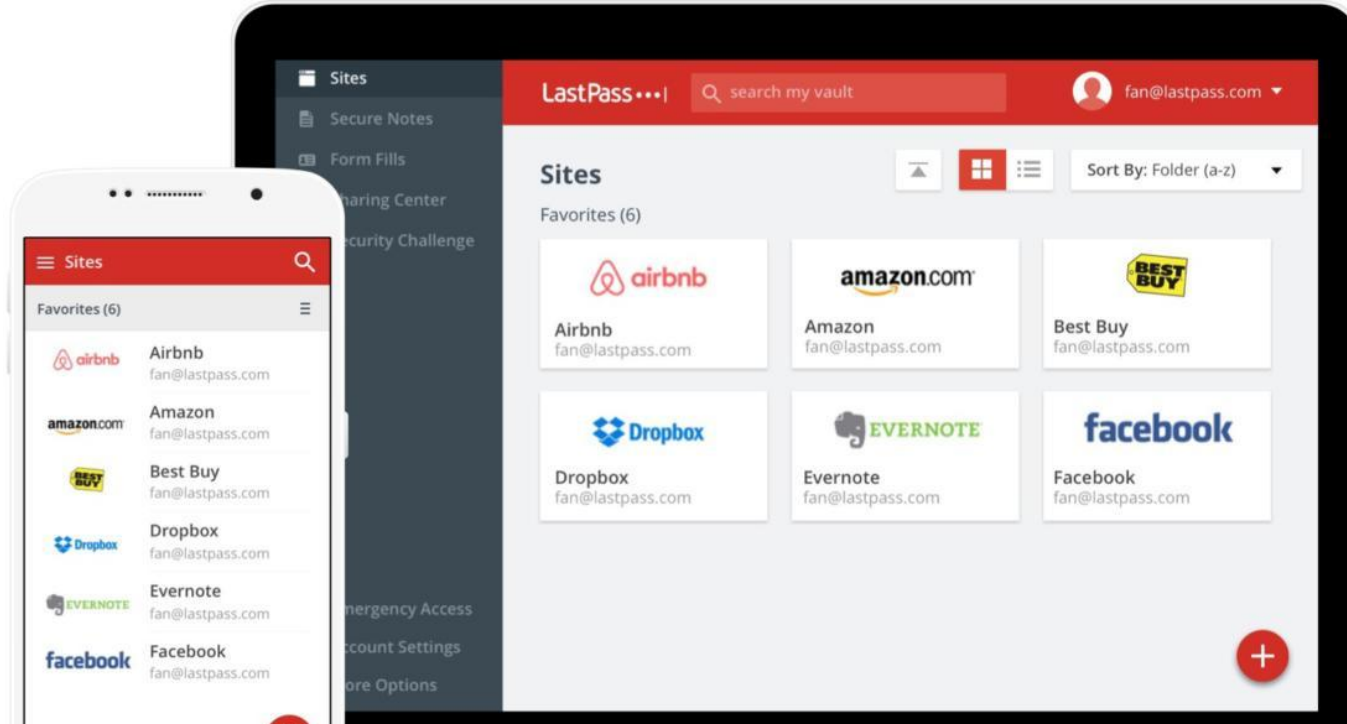
Here are four that are reliable:

- LastPass ([lastpass.com](https://lastpass.com))
- 1Password ([1password.com](https://1password.com))
- Dashlane ([dashlane.com](https://dashlane.com))
- Bitwarden ([bitwarden.com](https://bitwarden.com) - free & open source!)



# What's a password manager?

Password management services generate and hold diverse, strong passwords.



# Password Managers are Secure!

- Stored securely with end-to-end encryption (more on this later!)
- Generates random passwords
- Some password managers warn you when you have weak or reused passwords
- Enables safe sharing of sensitive information



# Password Managers are Convenient!

The image displays a password manager interface with three main components:

- Left Panel (Password Generator):** Features a "Back" button, a generated password "zZ4\$EAd5do\$U7r9gdIj% m1lApV@l\$G^NI", and a "SHOW HISTORY" link. Below is a "Password length" slider set to 43. On the right, there are four checked checkboxes: "Uppercase", "Lowercase", "Numbers", and "Symbols". On the left, there are three radio buttons: "Easy to say", "Easy to read", and "All characters" (which is selected). A red "FILL PASSWORD" button is at the bottom.
- Center Panel (Sign in page):** Shows the "LOGIN.GOV" logo at the top. Below it is the "Sign in" heading, followed by an "Email address" input field with a "2" character count icon. Below that is a "Password" input field. A "Log in as" dropdown menu is open, showing a globe icon and the text "login.gov" and "your.email@address.com".
- Right Panel (Update password dialog):** Titled "Update password?", it shows a preview of the password "airtable.com" and "your.email@a...". Below the preview, it says "I want to add a new account" and lists "LastPass" as a suggestion. There are three buttons: "Not now", "Update" (in red), and a "Cancel" button (partially visible).



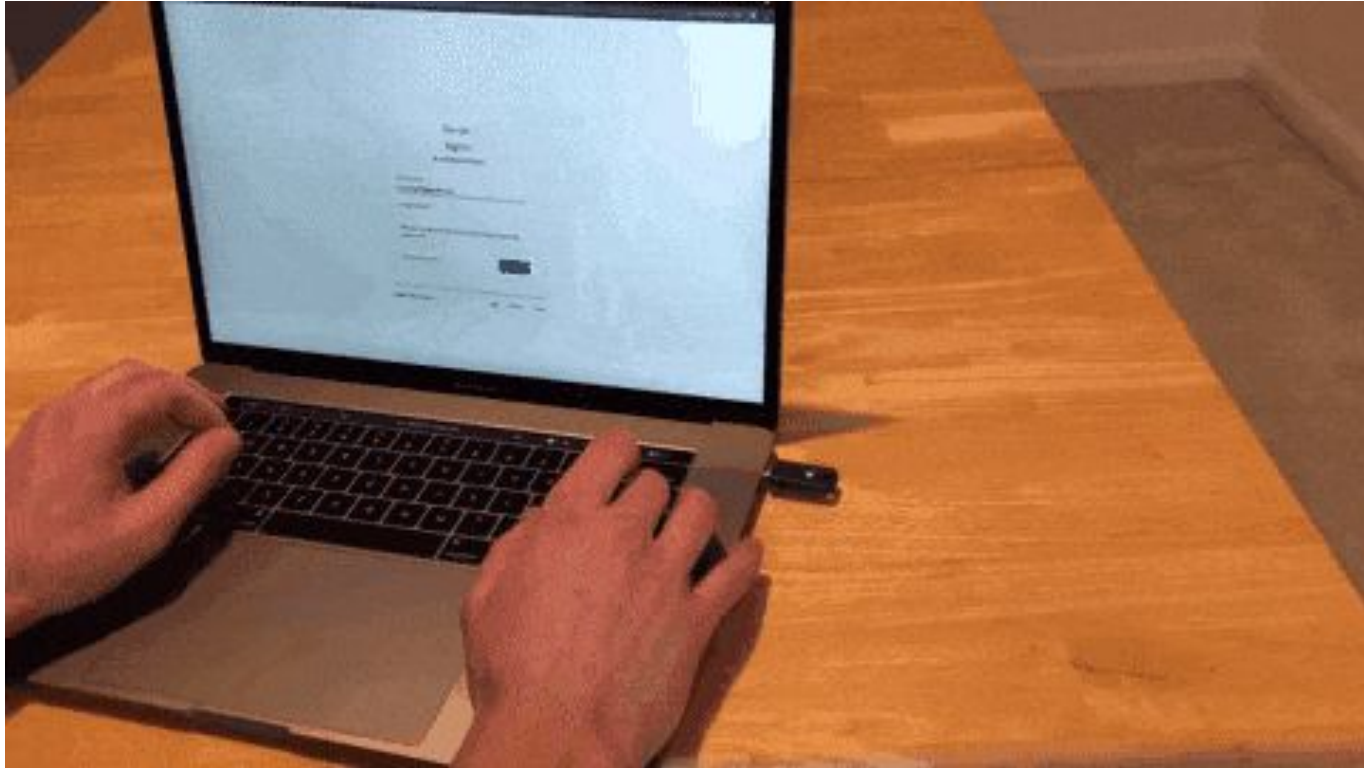
# Make an attacker need more than your password

“2 factor” or “multi-factor” authentication

- Something I know (a good password) = good
- Something I know + something I have with me = even better!

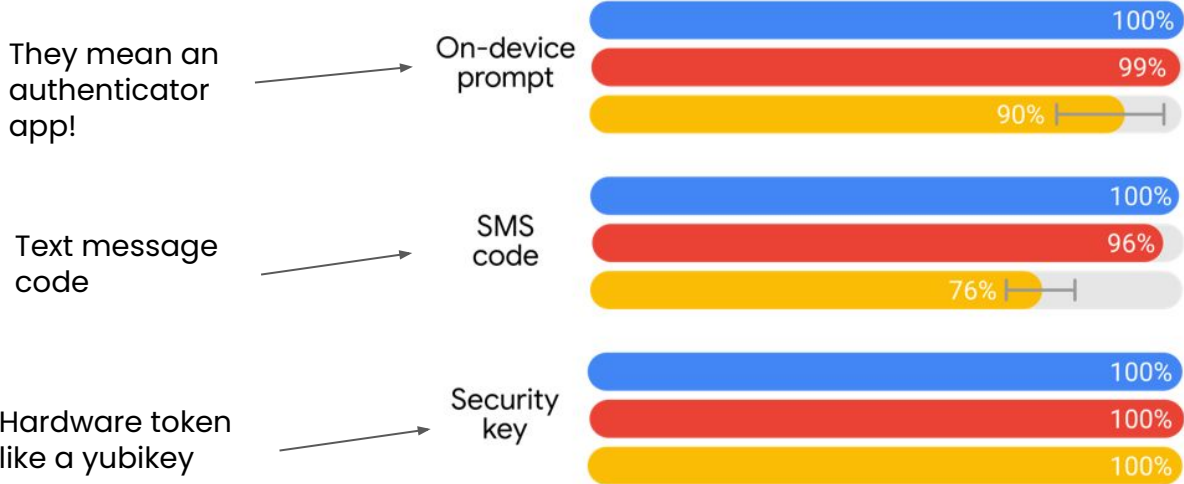


Illustration of security key from Solo (open source security key):



# How Effective is MFA? Account Takeover Prevention Rate

## Device-based challenges



They mean an authenticator app!

Text message code

Hardware token like a yubikey

On-device prompt

SMS code

Security key

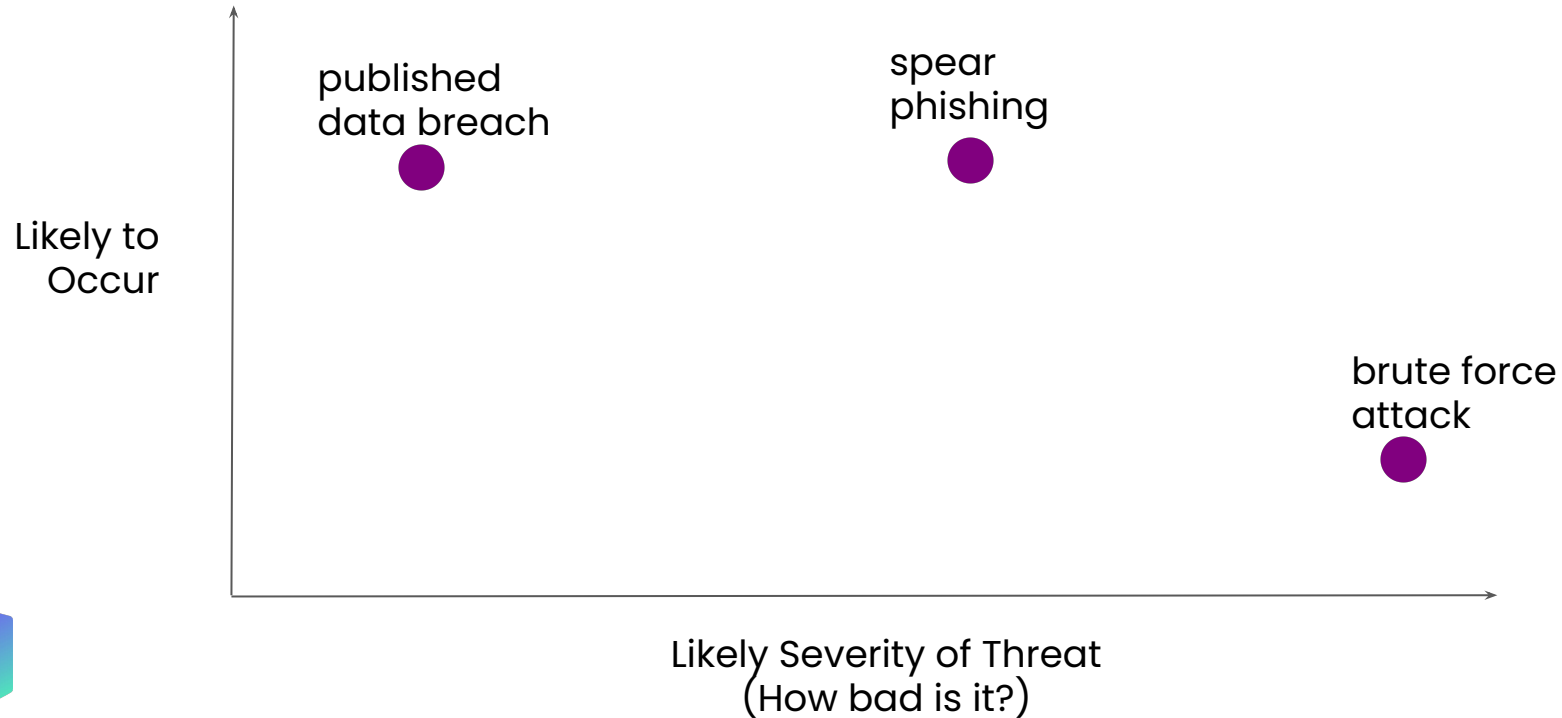


# Find step-by-step instructions:

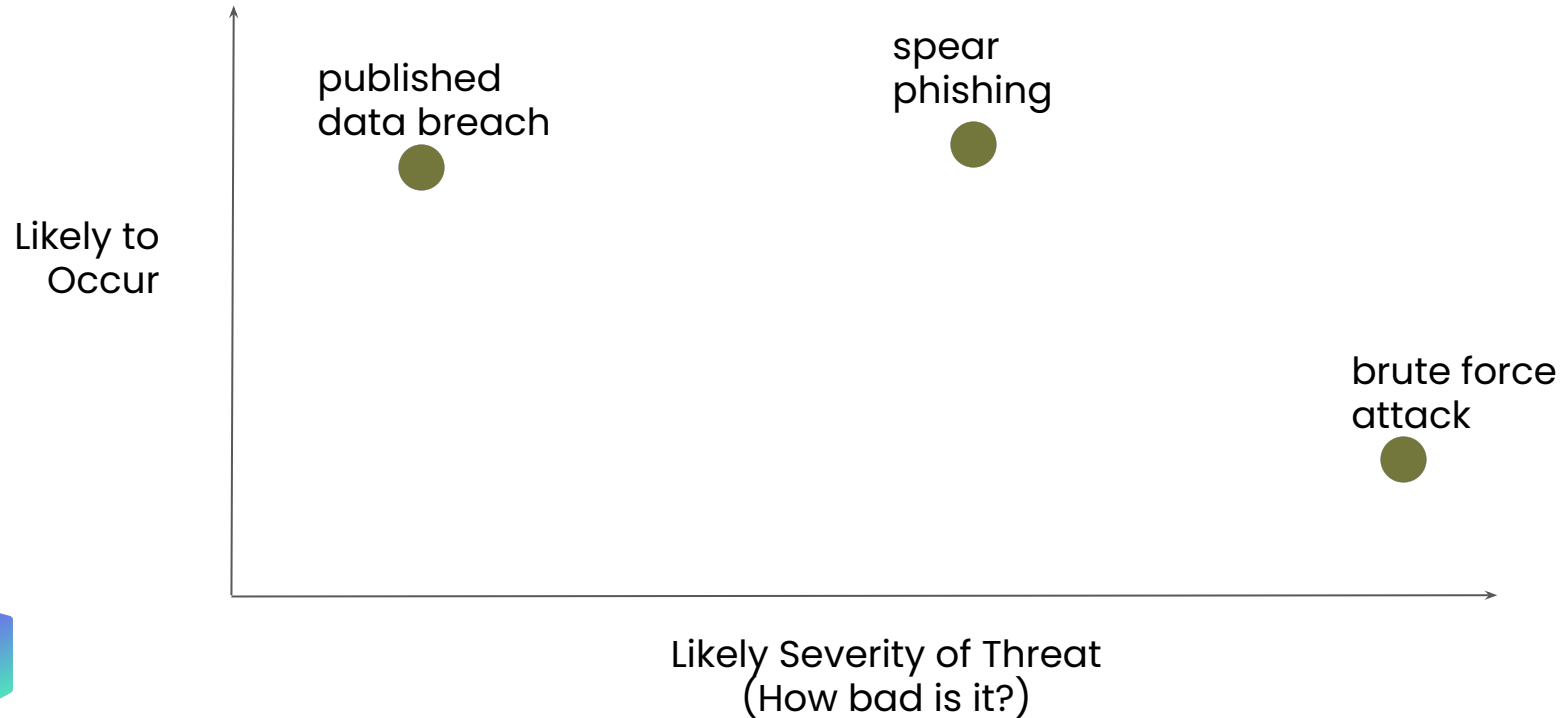
Get instructions for turning on 2FA for every account at [2fa.directory](https://2fa.directory)



# What threats can secure password practices (unique passwords & 2FA) prevent?



# What threats can secure password practices (unique passwords & 2FA) prevent?





## Follow-up:

Add 2FA to all the accounts you use in your work!

Each person using strong passwords and 2FA meaningfully improves the “herd immunity” of the entire organization to hacks and breaches.

## 2. Learn to identify phishing & email scam attempts





# What is phishing?

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

Phishing can also tempt you to download and install malware.

Source: Wikipedia



# What are phishing email scams?

Phishing can also simply try to get money or assets by disguising as a trustworthy entity in an electronic communication.

For email scams, the attacker doesn't even need your password! Often, they just try to pretend to be your boss or someone offering you an opportunity.



# Why do people phish?

- To get your password
- To get your money
- To get confidential information
- To get you to execute code or download malware on your computer



# Why does phishing work?

Phishers capitalize on our:

- Urge to be polite
- Urge to be helpful
- Fear of being embarrassed
- Panic about urgent messages

+ The only way to truly prevent it is to double check *everything* in another communication channel. We're too busy for that!!



# Examples of phishing:

You may have experienced these already!

## **No shame**

👉 Remember, people phish because it works, and it works because we're busy people who want to help people who contact us!



# The fake boss gift card scam

----- Forwarded message -----

From: [redacted]

Date: Tue, Jul 14, 2020 at 6:12 AM

Subject: Urgent

To: [redacted]

CC: [redacted]

Hi [redacted]

Visualizing my inner self-thinking of someone in the office who might be wonderful and honesty to run a personal errand for me. Imaging your accomplishments I pictured you. Kindly send me your cell and wait for my instructions.

Thanks

[redacted]

--

(This email was actually received by someone in our movement!)



---

**From:** [redacted] <[ashlynnDOBBS004@gmail.com](mailto:ashlynnDOBBS004@gmail.com)>

**Sent:** Monday, July 20, 2020 9:05 AM

**To:** [redacted]

**Subject:** INSTANT ASAP!!!

Hi Megan,

Would it be possible for you to complete a task for me before this conference ends ?

Please give me your personal number.

Thanks,

[redacted]

Sent from my iPhone.

(This email was actually received by someone in our movement!)



# Next step in the scam (if you take the bait)

**From:** [REDACTED]  
**To:** [REDACTED]  
**Subject:** RE: Vice President of [REDACTED] Task [REDACTED].  
**Date:** Tuesday, November 6, 2018 11:43:21 AM

---

OK! This is what I need is AMAZON GIFT CARDS OR GOOGLE PLAY GIFT CARDS of \$100 or \$200 face value. I need 20 of Each card. That's  $\$100 \times 20 = \$2000$ . Scratch the back out and Email me the codes or pictures of the codes. Let me know how soon you can get this done.

Regards  
Sent from my iPhone





# How do they do this?

- Use data from LinkedIn (breach or current profiles) or emails & organization structure scraped from website to figure out who is the boss & who reports to them
- Get an email & pretend to be the boss!
  - Make a new free email account with boss's name
  - Or use an email from a breach list and change the display name to the boss's name



# Remember those password breaches?

- They can be used to create pretty scary phishing scams!



Delete Not junk ▾ Block ...

## I know everything - proof

 This message was identified as spam. We'll delete it after 9 days. [It's not spam](#)



[Redacted]  
Sun 4/28/2019 12:35 AM

You ↵



Hi!

I know that: D3[Redacted]ld - is your password!

Also as you may have noticed, I sent this email from your email account (if you didn't see, check the from Sender email ID.)

I infected you with my private malware, RAT, (Remote Administration Tool) some time ago.

The malware gave me full access and control over your computer, meaning, I got access to all your accounts and I can see everything on your screen, even turn on your camera or microphone and you won't even notice about it.

I made a video showing both you (through your webcam) and the video you were watching (on the screen) while satisfying yourself!

I can send this video to all your contacts (email, social network)!



# Phishing for passwords: making fake login pages



## Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account  
[john.podesta@gmail.com](mailto: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

You received this mandatory email service announcement to update you about important changes to your Google product or account.





Mustafa Al-Bassam @musalbas · Sep 9, 2018

Quick phishing demo. Would you fall for something like this?

A screenshot of a legitimate Google account creation page in a Chromium browser. The address bar shows a secure connection to <https://accounts.google.com...>. The page features the Google logo, the text "One account. All of Google.", a profile icon placeholder, an "Enter your email" input field, a blue "Next" button, and a "Find my account" link. At the bottom, there is a "Create account" link and the text "One Google Account for everything Google". A video player overlay at the bottom left shows a progress bar at 0:06 and 485.1K views.

373 4.8K 7.9K



Mustafa Al-Bassam @musalbas · Sep 9, 2018

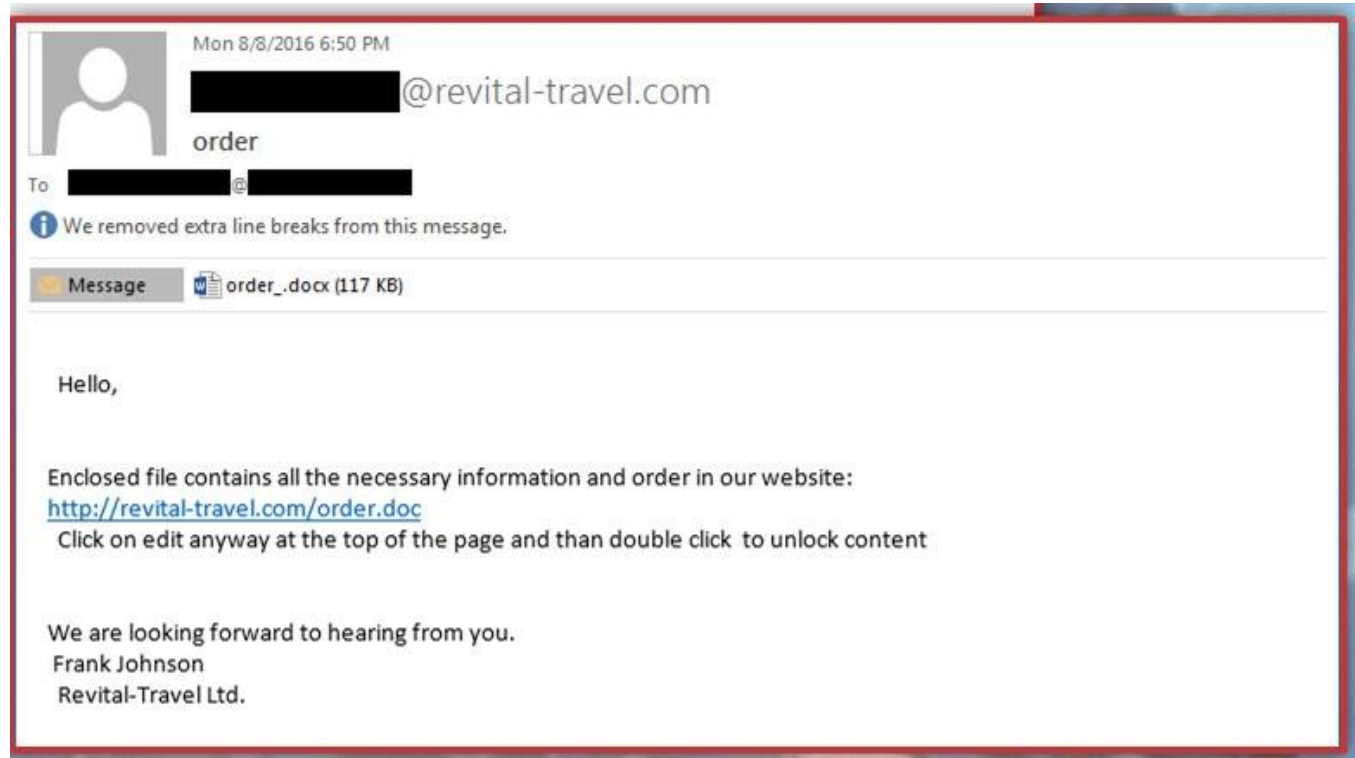
Quick phishing demo. Would you fall for something like this?

A screenshot of a phishing page designed to look like the legitimate Google account creation page. The address bar shows a secure connection to <https://accounts.google.com.secure.computer.shop/#i...>. The page content is identical to the legitimate page, including the Google logo, "One account. All of Google.", input field, "Next" button, and "Find my account" link. However, the page title in the browser tab is "demo.html" and the URL in the address bar is suspicious. A video player overlay at the bottom left shows a progress bar at 0:02 and 485.1K views.

373 4.8K 7.9K

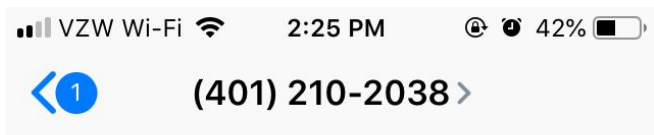


# Phishing to add malware to your device



<https://www.wired.com/story/fin7-wild-inner-workings-billion-dollar-hacking-group/>

# Not just emails: phishing texts, DMs, phone calls...



Text Message  
Today 2:19 PM

Hi Amanda, this is your delivery man. I was at your home earlier, but noone was at home. Confirm now: <http://8xuwajt.top/jpw6xw>

The sender is not in your contact list.

[Report Message](#)

"This confidential message is to inform you that you have a legal matter pending to be filed against you within the next 24 hours. You must call [PHONE NUMBER] and reference Case Number [FAKE CASE NUMBER]."



On the phone, the pressure to act quickly & be helpful can be even stronger!



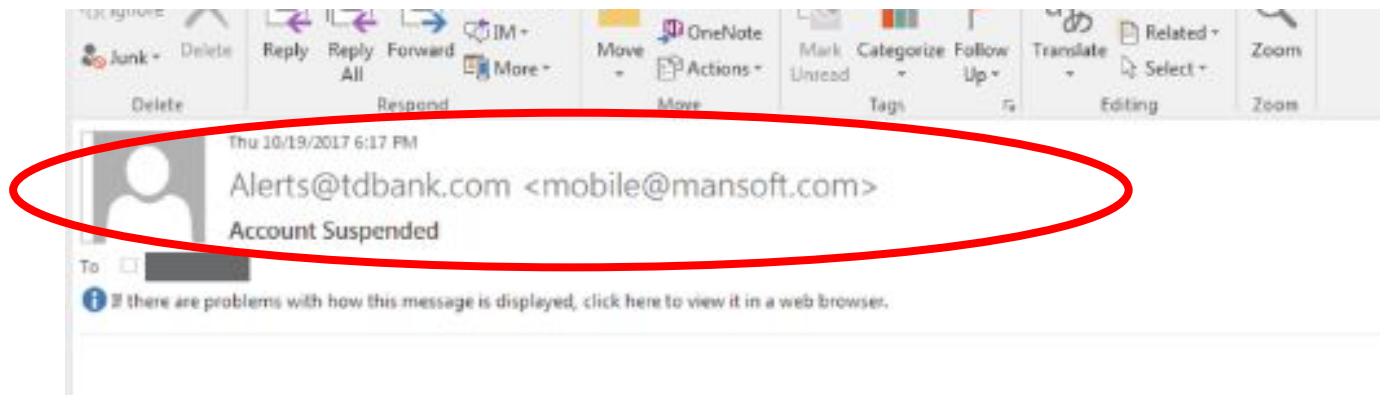


You can save time (and not have to double check a communication!) by recognizing a scam right away.

To further muddy the waters: Some legitimate emails will have these red flags. But it never hurts to double check those too!



# Red Flag: Who is the email from?



Note that on a mobile phone,  
only the first item will display!

# Red Flags: Who is the email to?

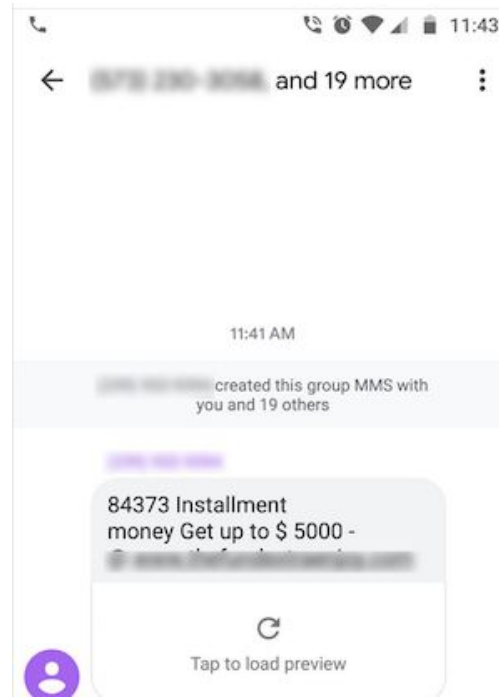
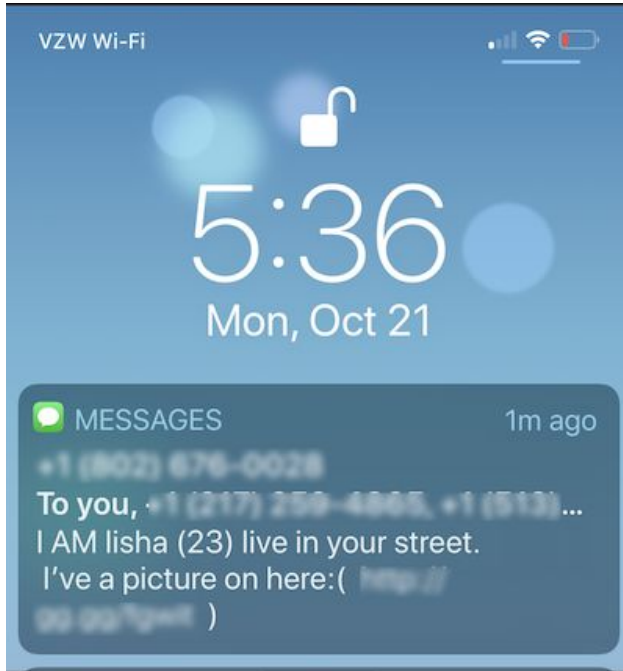


Image source: <https://www.komando.com/security-privacy/group-texting-from-neighbor-scam/606935/>

# Red Flag: Investigate hyperlinks!

- Hover over the linked text to see what the hyperlink really is
  - On a phone, tap and hold the linked text
- Look at each component of the hyperlink



# Know your URLs

https://www.google.com/path

Subdomain SLD TLD Path

HOST

### Second-level domain (SLD)

This is the part you can register and own. On www.google.com, google is the SLD. On safe.page, safe is the SLD.



# Know your URLs



https://www.google.com/path

Subdomain

SLD

TLD

Path

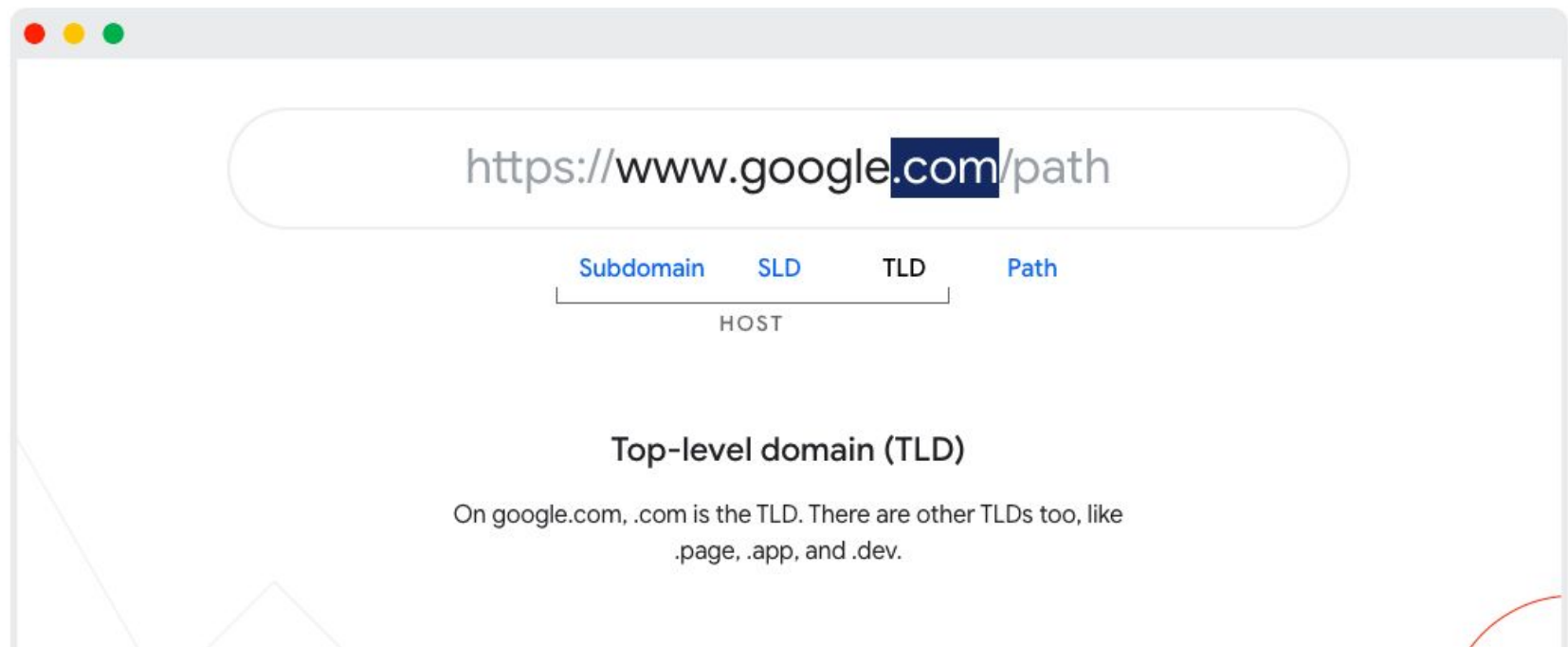
HOST

## Subdomain

Once you own an SLD, you can set up a subdomain (or several), like `blog.yourdomain.page` and `my.blog.yourdomain.page`.



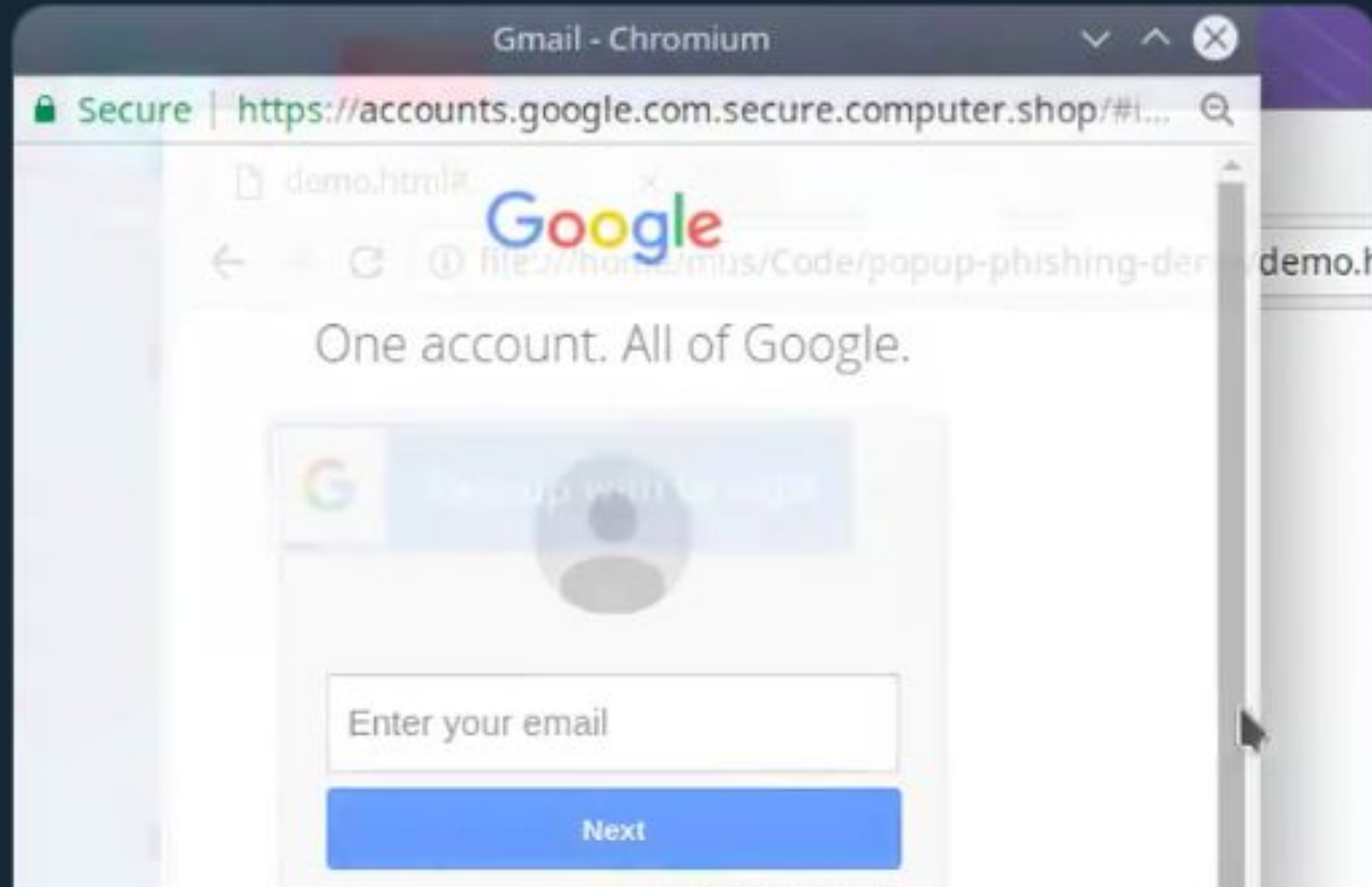
# Know your URLs





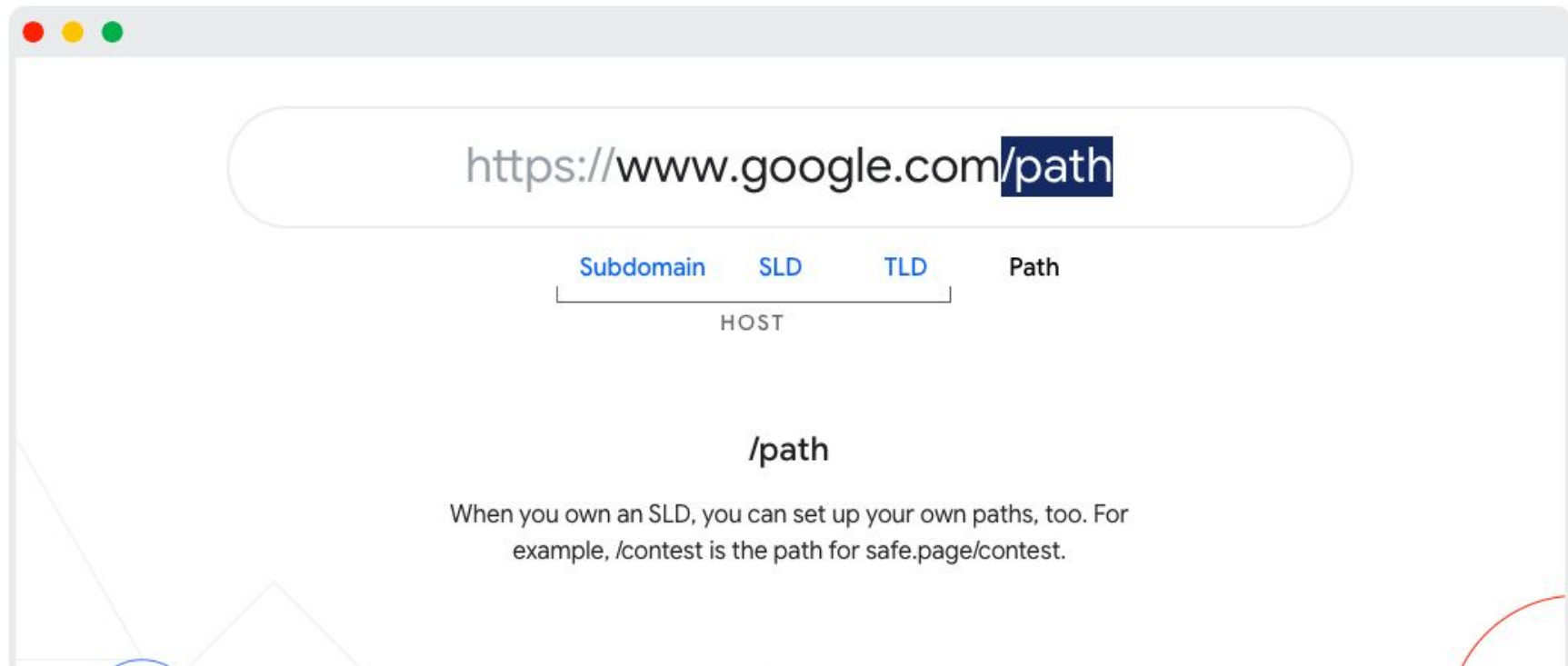
**Mustafa Al-Bassam** @musalbas · Sep 9, 2018

Quick phishing demo. Would you fall for something like this?






# Know your URLs



# Hyperlinks: there's another link in the link!

The image shows a Gmail notification from Google support. The sender is circled in red. The notification text includes a warning icon, a title, a paragraph of text, and a link. A red arrow points from the link in the text to a larger version of the same link in the footer, which is also circled in red.

Google <no-reply@google.support> to me ▾ 9:49 AM



**Government-backed attackers may be trying to steal your password**

There's a chance this is a false alarm, but we believe we detected government-backed attackers trying to steal your password. This happens to less than 0.1% of all Gmail users. We can't reveal what tipped us off because the attackers will take note and change their tactics, but if they are successful at some point they could access your data or take other actions using your account. To further improve your security, based on your current settings, we recommend:

[Change password](#)

<https://google.com/amp/tinyurl.com/y7u8ewlr>

<https://google.com/amp/tinyurl.com/y7u8ewlr>



# Trace Results

*Date Traced: 2021-02-23 17:47:21 GMT*

---

<http://google.com/amp/tinyurl.com/y7u8ewlr>

**301 Redirect**

<http://www.google.com/amp/tinyurl.com/y7u8ewlr>

**301 Redirect**

<https://www.google.com/amp/tinyurl.com/y7u8ewlr>



**302 Redirect**

<https://www.google.com/url?q=http://tinyurl.com/y7u8ewlr>



**Trace Complete - Total Redirects:3 -**



WhereGoes - Trace Results

## Trace Results

*Date Traced: 2021-02-23 17:45:06 GMT*

---

<http://tinyurl.com/y7u8ewlr>



**301 Redirect**

<http://jigsaw.google.com/>

**301 Redirect**

<https://jigsaw.google.com/>

**Trace Complete - Total Redirects:2 -**



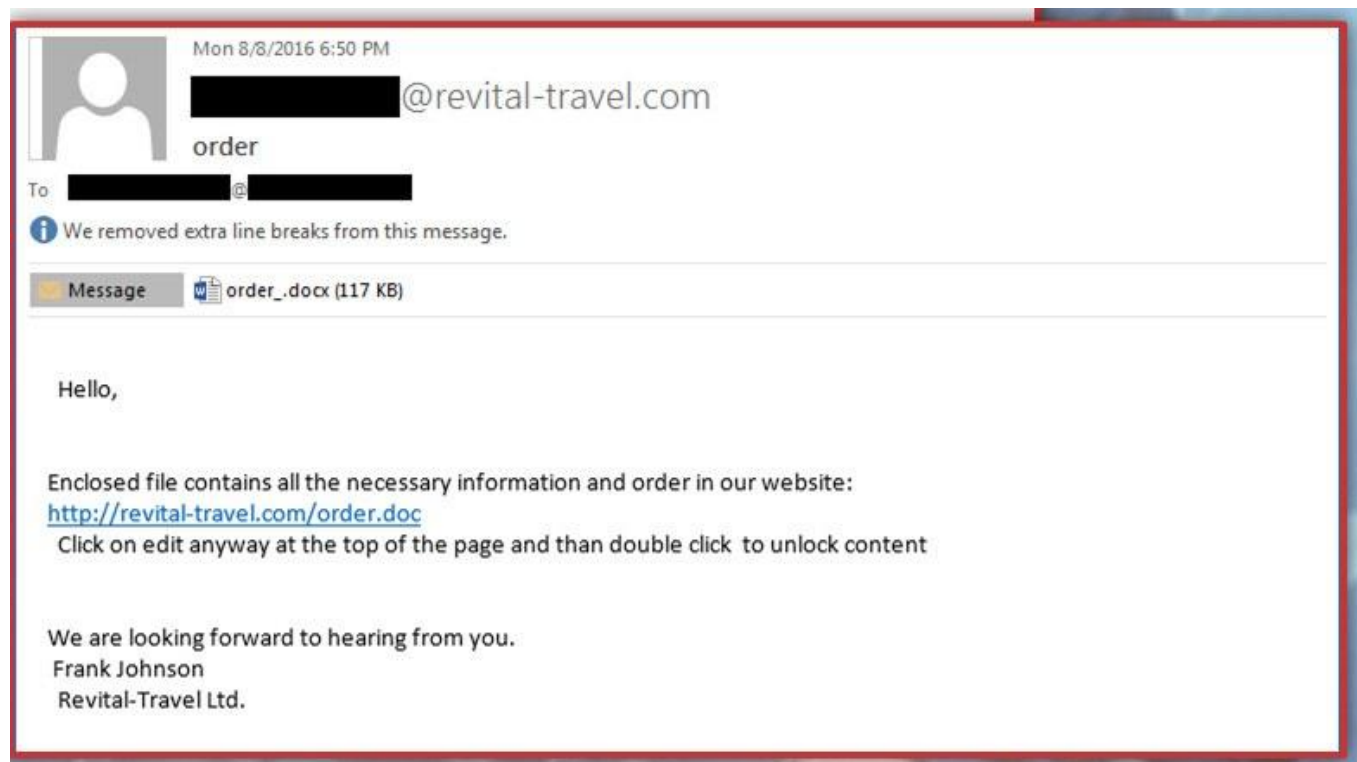
# Red Flags: Unexpected attachments

Unless you expected an attachment, an attachment is always a red flag!!

- Are you instructed to enable editing or otherwise take action with the document?



# Attachment: instruction to unlock content



<https://www.wired.com/story/fin7-wild-inner-workings-billion-dollar-hacking-group/>



# Red Flag: Urgency, extortion, or money

It's always worth it to double check or get help with emails that:

- Threaten you
- Ask for money
- Present an urgent need you didn't anticipate

Do a gut check, and slow down!



# Prevent phishing:

- Change norms: Reaching out to a peer organization or colleague to confirm the email is both appropriate and effective.
- Keep your email private.
  - Spear phishers scrape emails from websites so keep your email off your website, workplace's website, and social media accounts.
- Slow down!
- Trust your gut.
- Learn to recognize the signs and always double check for them...





# If you suspect phishing

- DO NOT CLICK!
  - Do not click on links!
  - Do not open attachments!
  - Do not enable editing!
  - If you haven't already, don't open the email!
- If it's (supposedly) from someone you know:
  - Text or call to verify
- If it's from someone you don't know:
  - Take a screenshot and send to a manager at work



# If you do click and realize something is wrong...

- Tell someone else at your organization immediately!
  - Even if it looks like nothing bad happened, attackers can be carrying out malicious activity in the background like...
    - Sending spam emails from your account
    - Reading/monitoring your email
    - Changing details on your account
- Monitor your account's activity
  - Check the access logs
  - Check sent & deleted messages
  - Check for forwarding rules
- Change your password!





## Follow-up:

Create a plan for reporting suspected phishing emails at your organization.

- Who should people forward an email or screenshot to if they suspect they've been targeted?
- Who should people contact if they clicked on an email and then realized something was wrong?

# 3. Access Controls: Who Has Access to What?

# The responsibility of protecting data is shared between platforms and users

## What they control:

- Security of our data in transit
- Security of our data storage
- What and how they share our data with other services, or entities

## What we control:

- Our login
- What and how we share with other services
- **What and how we share with other users**
- Our devices we use to access those platforms

# Only create accounts for or share access with people who need it.

- Slack
- GSuite/Google Drive
- Instagram/social media accounts
  - Tip for social media accounts that must be shared:
    - Share passwords with a password manager so access can be revoked
    - Consider using Tweetdeck teams to manage shared Twitter accounts, so that each person can have their own secure login
    - Use Facebook Business Manager to manage Instagram content so everyone can use their individual secured Facebook accounts to access Instagram (instead of sharing a password)

# Most cloud software make access control easy!

- Familiarize yourself with the permissioning features on accounts you manage
  - Ex: Slack
    - Private channels
    - Public channels
    - Shared channels
    - Guest accounts
  - Ex: GSuite/Google Drive
    - Shared drives
    - Share via email invite (instead of sharing a link)



# Keep track of who is coming & going!

- Include all organization & coalition accounts in an onboarding & offboarding checklist.
- Communicate with coalitions about new staff members who need to be given access, and leaving staff members who needs to have access removed.
  - Tip: Create a Google form to request adding or removing access to coalition accounts, which sends a notification to the person who holds the admin privileges to add or remove people!



# Access Control Tactics

- Limit the number of people who have access to sensitive accounts.
- Review access logs for red flags or unauthorized access.
- Regularly audit user & admin lists for Slack, GSuite, Facebook, etc.
- Require use of institutional email under your organization's administrative control.



## Follow-up:

Review the workspaces you use or share.

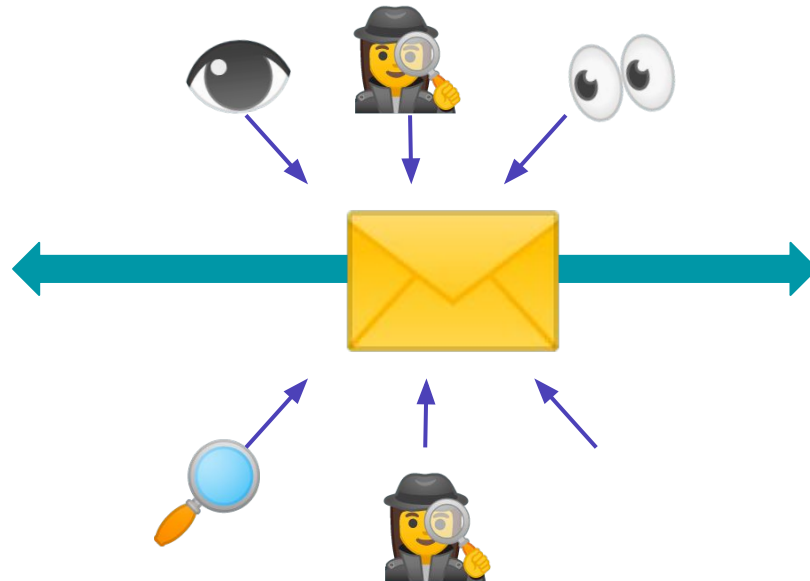
Can you enforce 2FA for everyone who has an account?

Are there any documents no longer in use, or old projects you can delete, disable sharing, or remove collaborators who no longer work there?

# 4. Encryption

# What is encryption?

- Encryption uses math to scramble your data
- The data can only be unscrambled with your private key



# The responsibility of blocking those actors is shared between platforms and users

What they control:

- **Security of our data in transit**
- **Security of our data storage**
- What and how they share our data with other services, or entities

What we control:

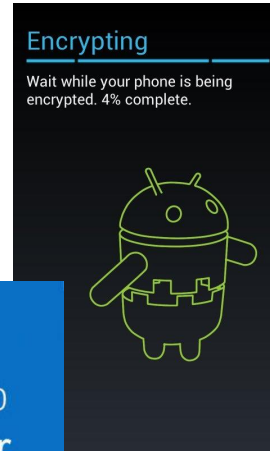
- Our login
- What and how we share with other services
- What and how we share with other users
- **Our devices we use to access those platforms**

# We can encrypt our devices

- Protect the data on your devices in the case of loss or theft



FileVault for Macs



BitLocker for Windows



Phones encrypted by default with passcode or PIN



# We can choose platforms that encrypt our data.

When data is encrypted, only the people with the encryption key can read it!

There are two main ways that companies can encrypt our data:

- In transit & at rest
- End-to-end

## In transit/at rest

- The company owns the encryption keys
- Company can decrypt your data if they want to or if they are asked to show it

Example: Slack, GSuite, Microsoft 365, Canva, Instagram

## End-to-end encryption

- Aka “zero knowledge”
- You own the encryption keys!
- The company cannot decrypt your data

Example: Signal, Protonmail





# The responsibility of blocking those actors is shared between platforms and users

## What they control:

- Security of our data in transit
- Security of our data storage
- What and how they share our data with other services, or entities
- **To respond to legal requests & self-monitor for use of the platform for crime**

## What we control:

- Our login
- What and how we share with other services
- What and how we share with other users
- Our devices we use to access those platforms

# The responsibility of blocking those actors is shared between platforms and users

## What they control:

- Security of our data in transit
- Security of our data storage
- What and how they share our data with other services, or entities
- **To respond to legal requests & self-monitor for use of the platform for crime**

## What we control:

- Our login
- What and how we share with other services
- What and how we share with other users
- Our devices we use to access those platforms
- **What potentially legally-sensitive info we store, or not, on the platform**

Remember:  
encryption does  
not mean you  
are 100%  
anonymous or  
secure!



SwiftOnSecurity  
@SwiftOnSecurity



When you reuse your MySpace  
password on your ProtonMail  
account



5:45 AM · 2/23/19 · [Twitter for iPhone](#)



## Follow-up:

Decide what conversations with collaborators should move from platforms like Slack to end-to-end encrypted platforms like Signal.

Write down who you talk with the most about these items, and invite them to connect on Signal after this training.

# 5. Data Retention



# The responsibility of protecting data is shared between platforms and users

## What they control:

- Security of our data in transit
- Security of our data storage
- What and how they share our data with other services, or entities

## What we control:

- Our login
- **What and how we share with services**
- What and how we share with other users
- Our devices we use to access those platforms



# What is a data retention policy?

- Details how, where, and how long data is stored

# What is included in a data retention policy?

- Emails and other electronic documents
- Spreadsheets
- Contracts
- Correspondence between staff and clients, agents, vendors, shareholders and the public
- Employee/volunteer records
- Donor records
- Any applicable sales, invoice and billing info
- Tax and accounting documentation
- Financial reports
- Healthcare and patient data
- Student and educational data
- Any other data produced, collected and maintained in regular business activities



How long should we keep data?

**It depends!**

# How long should we keep data?

## Sample IRS rules:

- Forever
  - application for recognition of tax-exempt status
  - IRS determination letter
  - articles of incorporation and bylaws
  - board minutes.
- Four years
  - Employment Tax Records
- Three years
  - records that support an item of income or deduction on a return
  - three years is the general statute of limitations for returns, but state or local tax purposes may require longer retention



# How long should we keep data?

## Sample

- For  
  - 
  - 
  - 
  -
- For  
  -
- Three years  
  - records that support an item of income or deduction on a return
  - three years is the general statute of limitations for returns, but state or local tax purposes may require longer retention

As laws and regulations can vary from state to state and depending on service types, it is essential for your org to seek expert legal help to find out what you have to keep!



## Follow-up:

Do you need help composing a data retention policy? Work together to ask questions like:

- Is there a legal obligation to keep this data?
- Would a breach of this data harm people?
- Do we need this data for our operations or reporting?
- Do we need ALL of this data for our operations or reporting?
- Can we make this data anonymous?

And then document for your team to use and update.

Remember as digital security  
can feel tedious and abstract...  
data = people!  
When we protect our data, we  
protect our communities.

# People bring their (negative) experiences with surveillance to their interactions with your organization.

- Do people you work with understand how you got their information?
- Are you able to explain to the people you work with why you collect the information you do?
- Could the information you store about people be dangerous if it fell into the wrong hands?

# With our follow-ups we can flip the script, and be leaders in best data practices.

- We can help clients, donors, volunteers, understand how we got their information, and what policies we use in handling it.
- We can proactively agree with our partners on best practices to work together, and help collectively maintain data hygiene.
- We can rely on our teams to ensure there are many eyes and hands on the day-to-day work of looking out for everyone's privacy.