DIGITAL SECURITY IS FOR EVERYONE
PART ONE

Shannon Turner

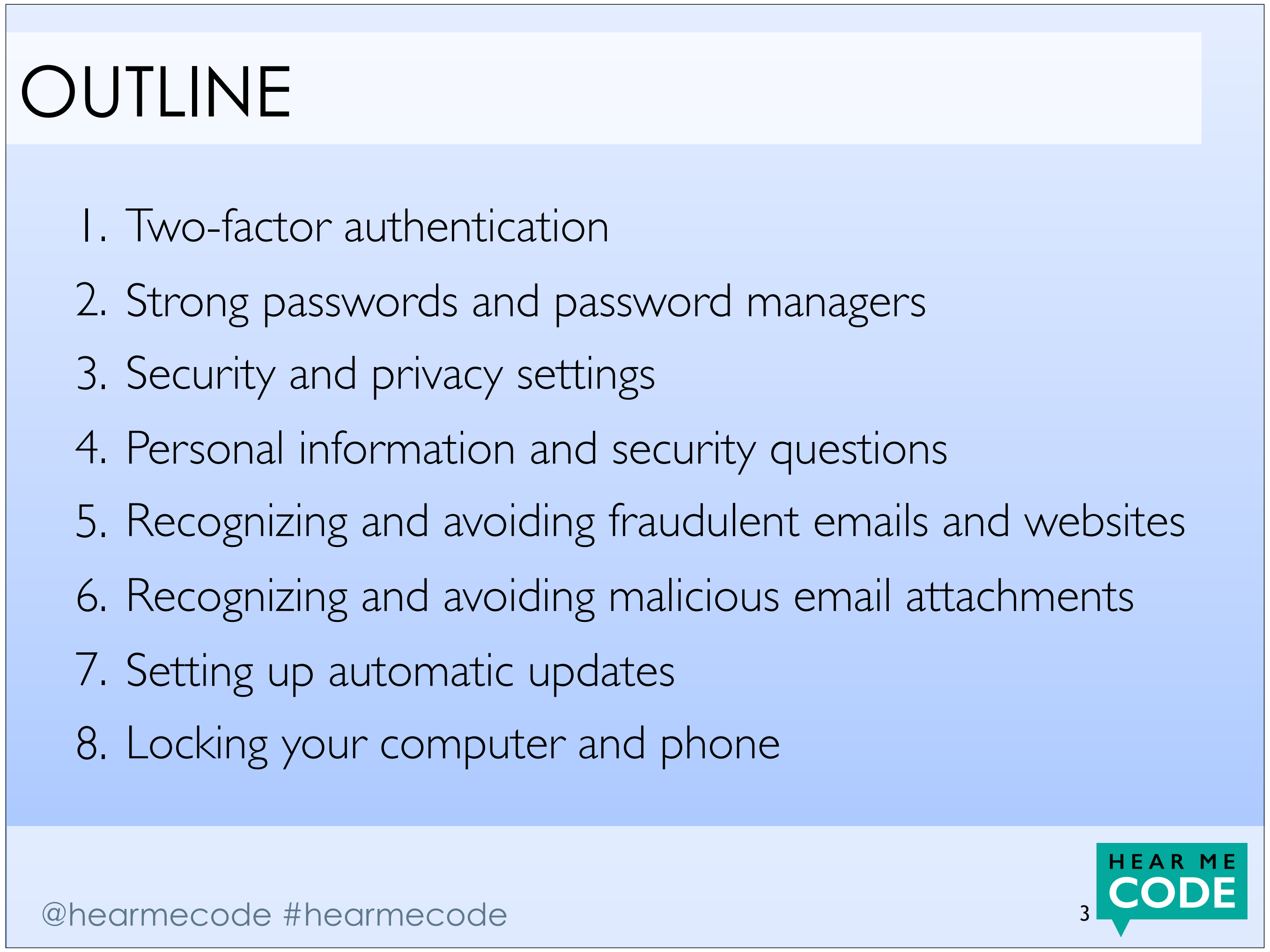
Twitter: @svthmc

This training was created for people who are not sure how to protect themselves online but want to know how to get started.

OBJECTIVE

- Learn how to recognize threats to your computer, your accounts, and your personal information
- Learn the most impactful practices and tools you can use to keep your accounts and information safe

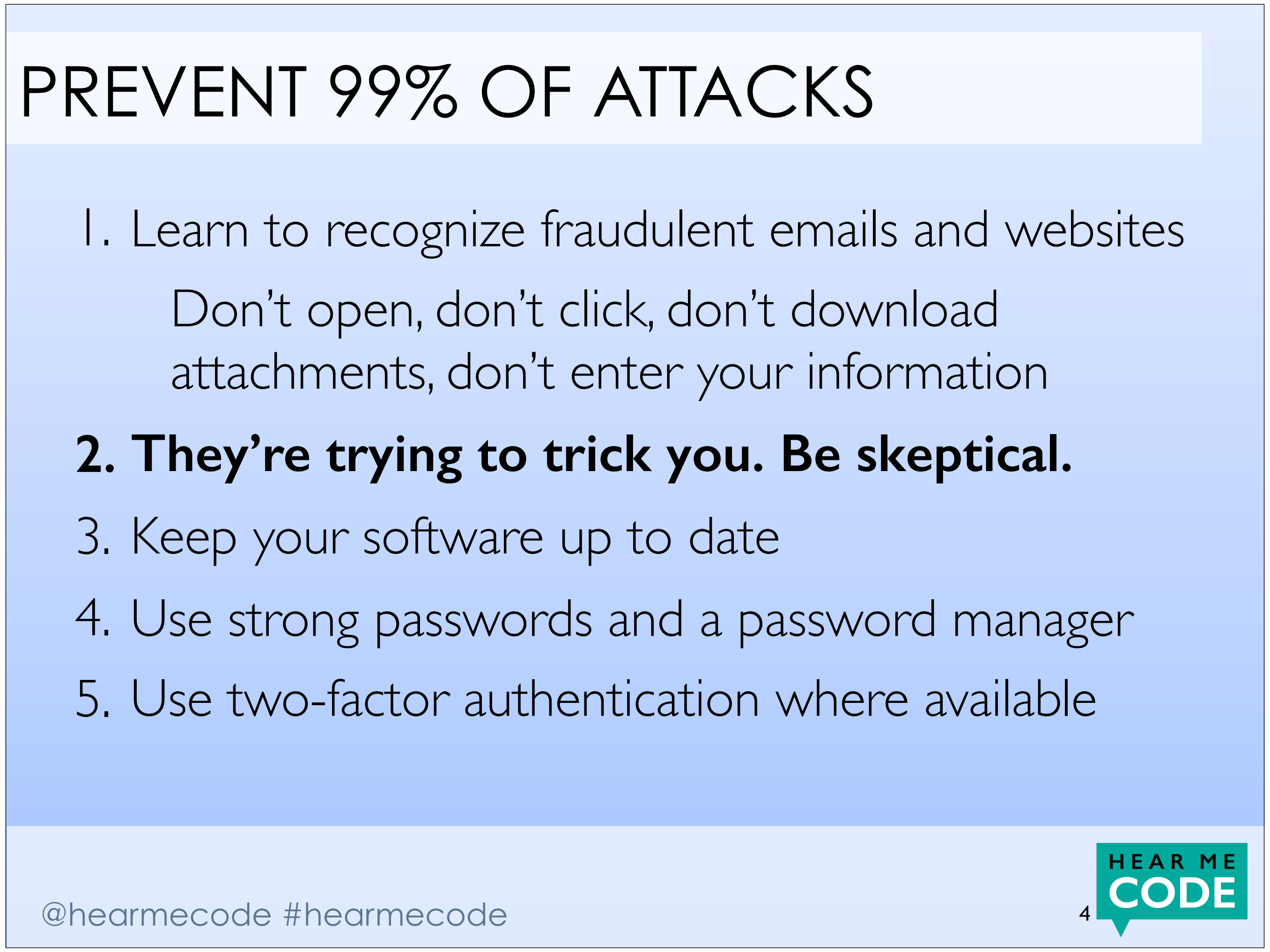
It’s important to note that this should be considered an intro training. This does not cover every single thing you will need to do or can do. We will not talk about every threat. We will cover the most common threats and how you can protect yourself. This training is meant as a starting place, especially if you’ve never thought too much about how to protect yourself.



OUTLINE

1. Two-factor authentication
2. Strong passwords and password managers
3. Security and privacy settings
4. Personal information and security questions
5. Recognizing and avoiding fraudulent emails and websites
6. Recognizing and avoiding malicious email attachments
7. Setting up automatic updates
8. Locking your computer and phone

These are the main topics we'll be covering during this training. A big part of this training is showing you how to recognize what emails and websites are legitimate and which are not. Learning these skills is just as important as using the right tools.



PREVENT 99% OF ATTACKS

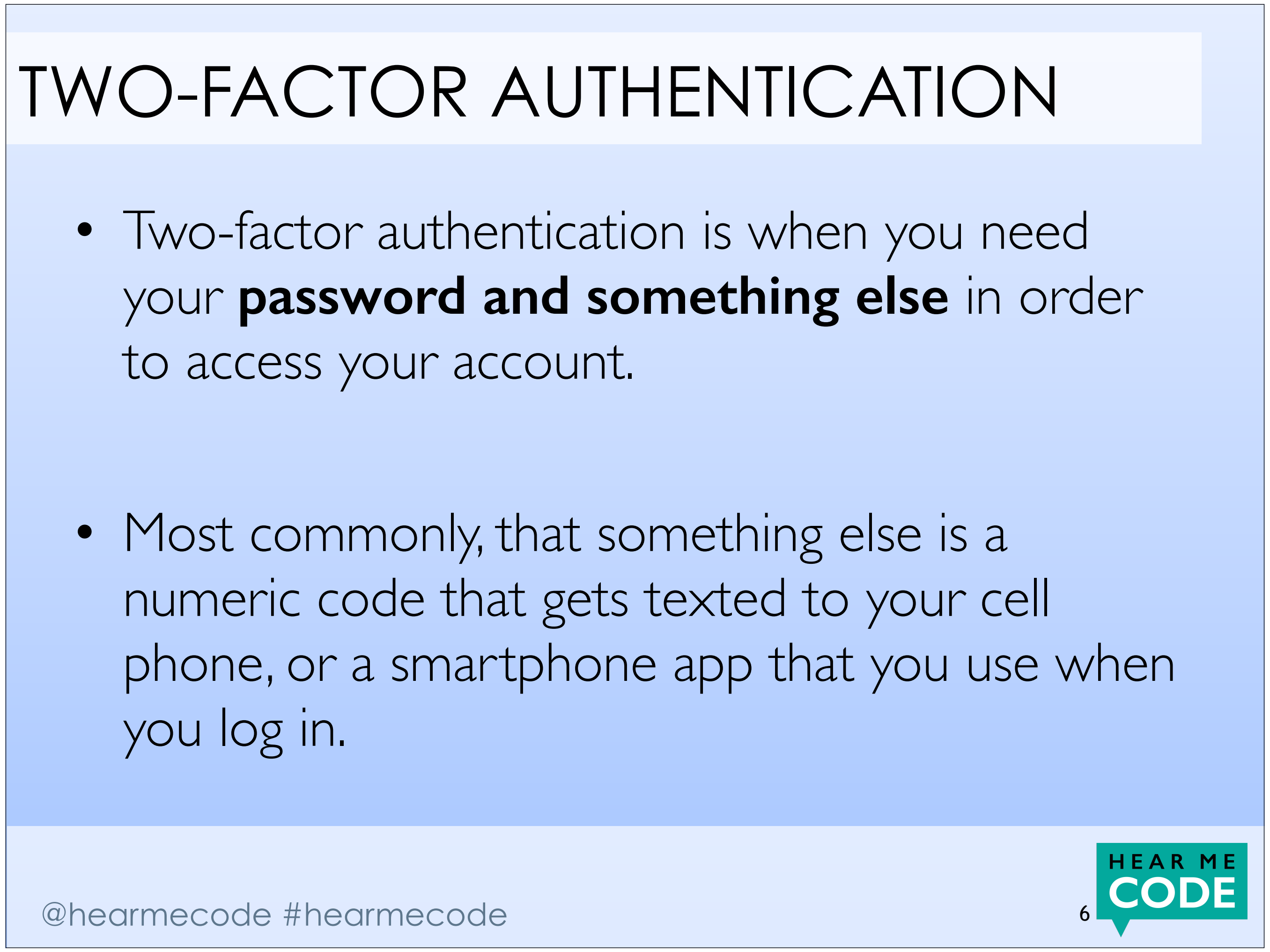
1. Learn to recognize fraudulent emails and websites

   Don't open, don't click, don't download attachments, don't enter your information

2. **They're trying to trick you. Be skeptical.**
3. Keep your software up to date
4. Use strong passwords and a password manager
5. Use two-factor authentication where available

With these five steps, we're going to learn how to protect ourselves from 99% of the most common threats.

TWO-FACTOR AUTHENTICATION



TWO-FACTOR AUTHENTICATION

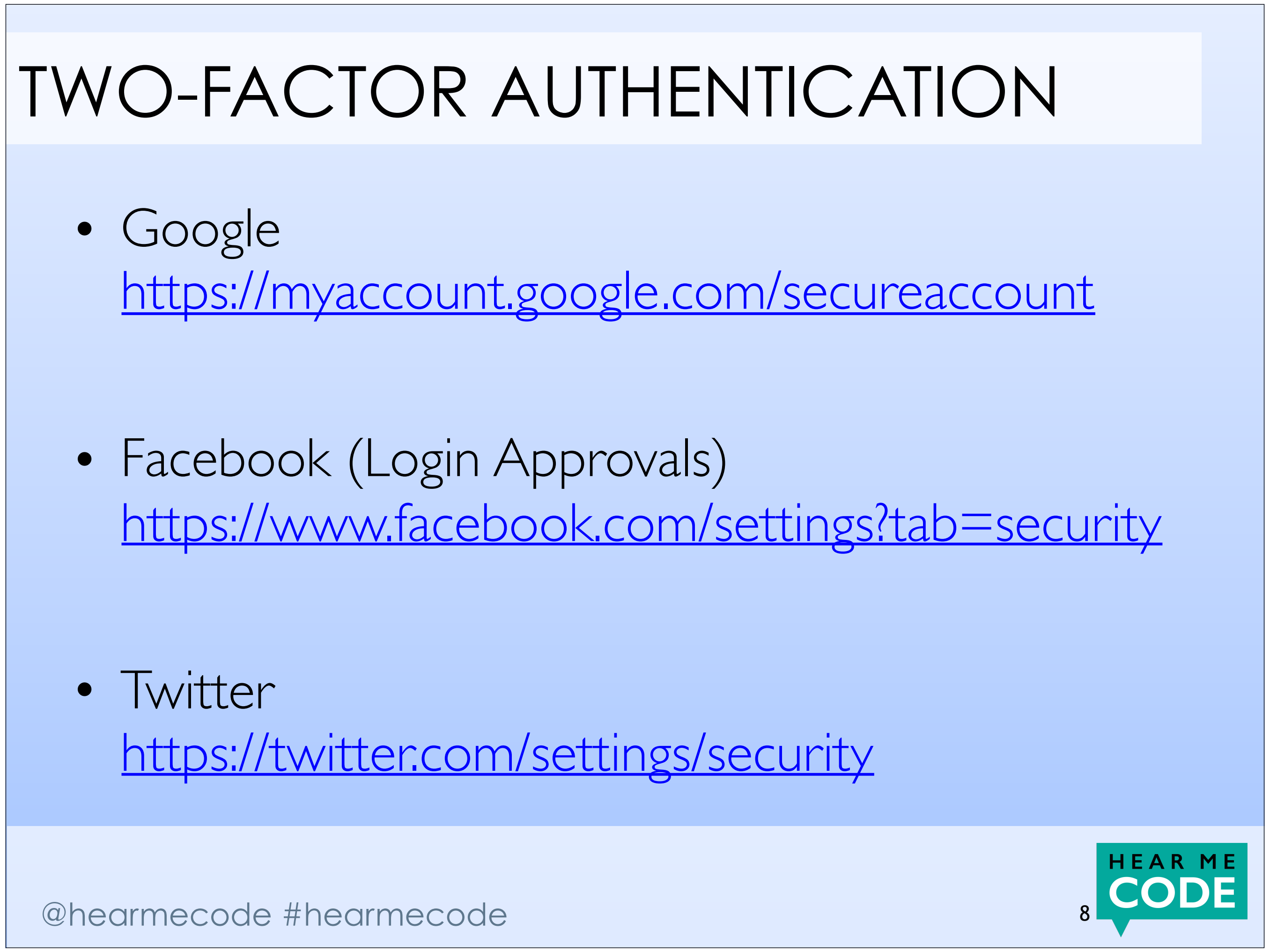
- Two-factor authentication is when you need your **password and something else** in order to access your account.
- Most commonly, that something else is a numeric code that gets texted to your cell phone, or a smartphone app that you use when you log in.

Setting up two-factor authentication to send you an SMS code is good but Authenticator apps are more secure.

TWO-FACTOR AUTHENTICATION

- Two factor authentication is **one of the best ways to secure your accounts.**
- **Even if someone got your password, they wouldn’t be able to get in** unless they also had your cell phone.

There are other ways to do two-factor authentication beyond SMS and smartphone apps like USB keys, but we won’t talk about those here.



TWO-FACTOR AUTHENTICATION

- Google
  https://myaccount.google.com/secureaccount
- Facebook (Login Approvals)
  https://www.facebook.com/settings?tab=security
- Twitter
  https://twitter.com/settings/security

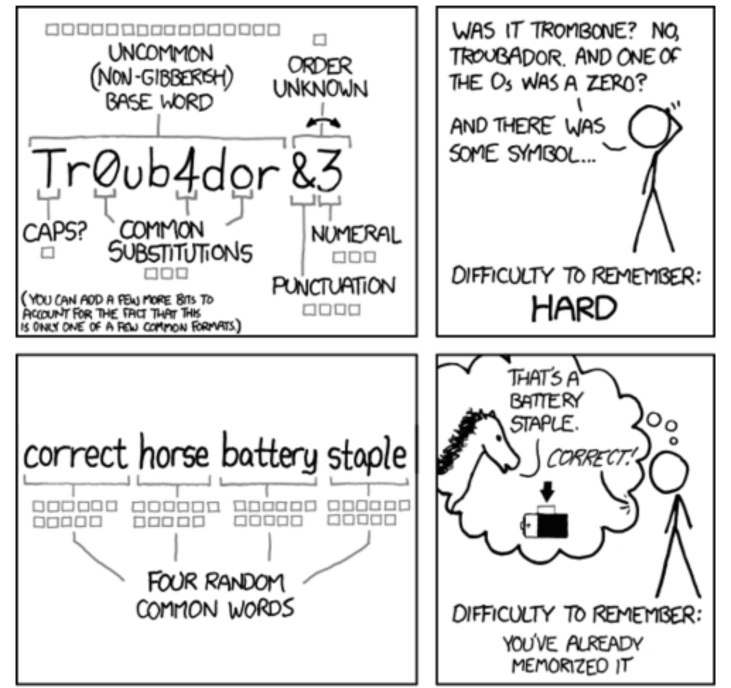
Here are the links to set up two-factor authentication for Google, Facebook, and Twitter. Many programs and services offer two-factor authentication, not just these three, and you should use it whenever and wherever it's available. You'll also want to review the other security and privacy settings on these pages too.

STRONG PASSWORDS & PASSWORD MANAGERS

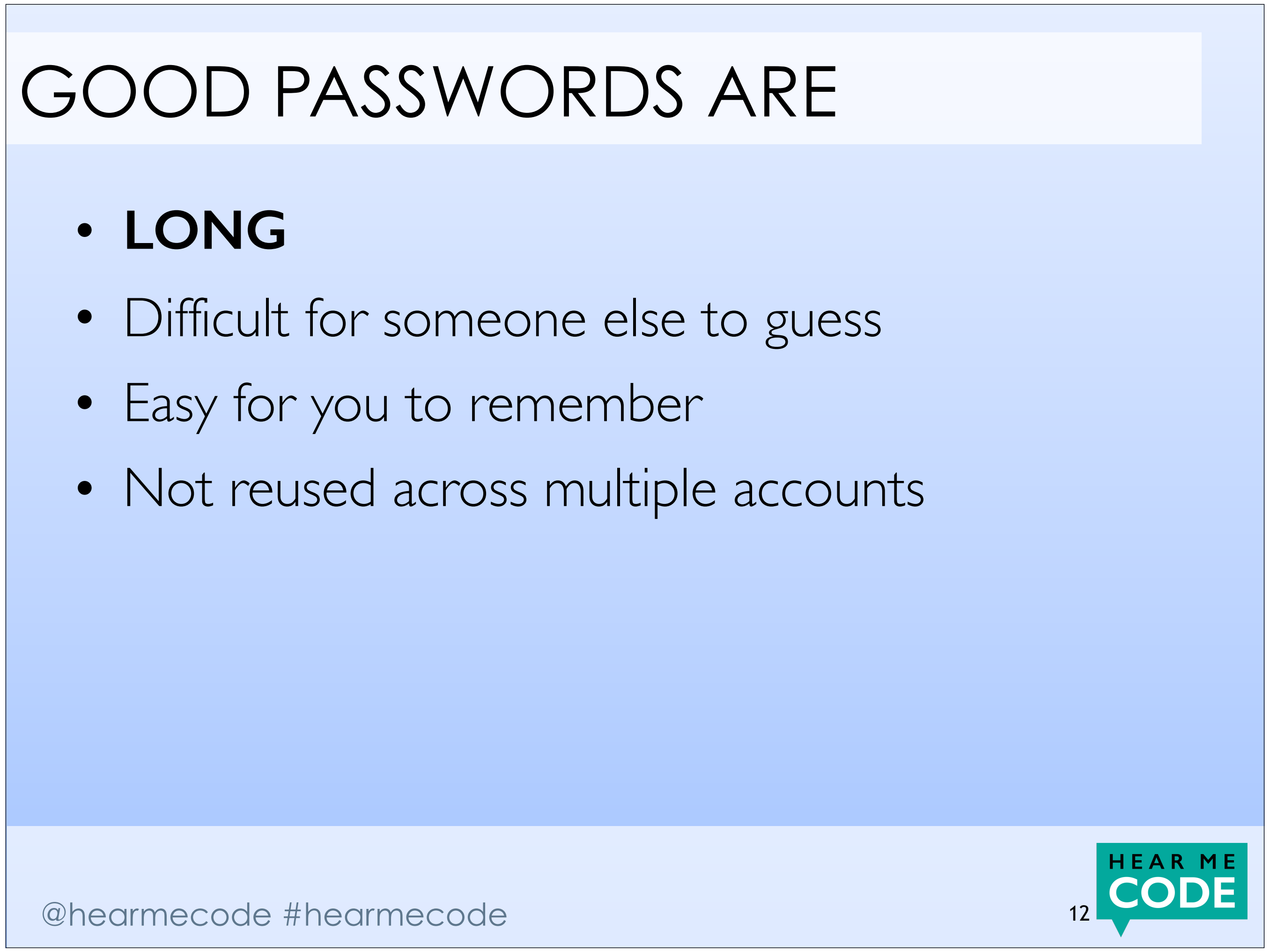
PASSWORDS ARE IMPORTANT

- Even if you have two-factor authentication enabled, make sure you are using strong passwords!
- But what makes for a strong password?

ADAPTED FROM XKCD.COM/936


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

This comic pokes fun at passwords. A lot of accounts force you to add numbers, symbols, and capital letters to your passwords to make them "stronger" but that often just makes them harder to remember without making them more secure. The most secure passwords are very long and easy to remember.

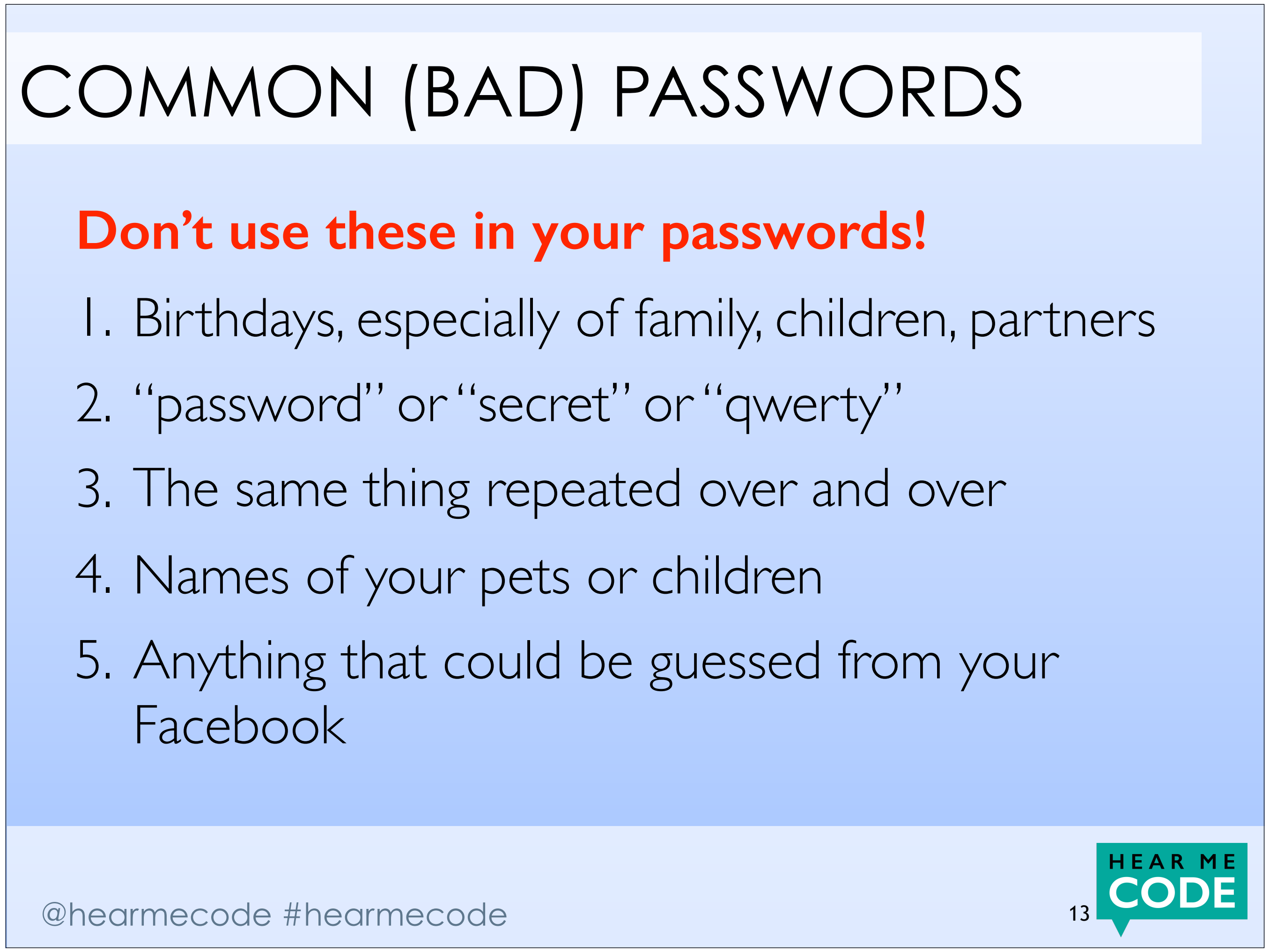


GOOD PASSWORDS ARE

- **LONG**
- Difficult for someone else to guess
- Easy for you to remember
- Not reused across multiple accounts

Why can’t you re-use passwords? Let’s say I use the same password for my email and for my online banking. If someone got the password to my email, they could also get into my bank account.

If you can’t reuse passwords, it can be challenging to create long, secure passwords unless you use a password manager. We will talk about password managers in a couple of slides.

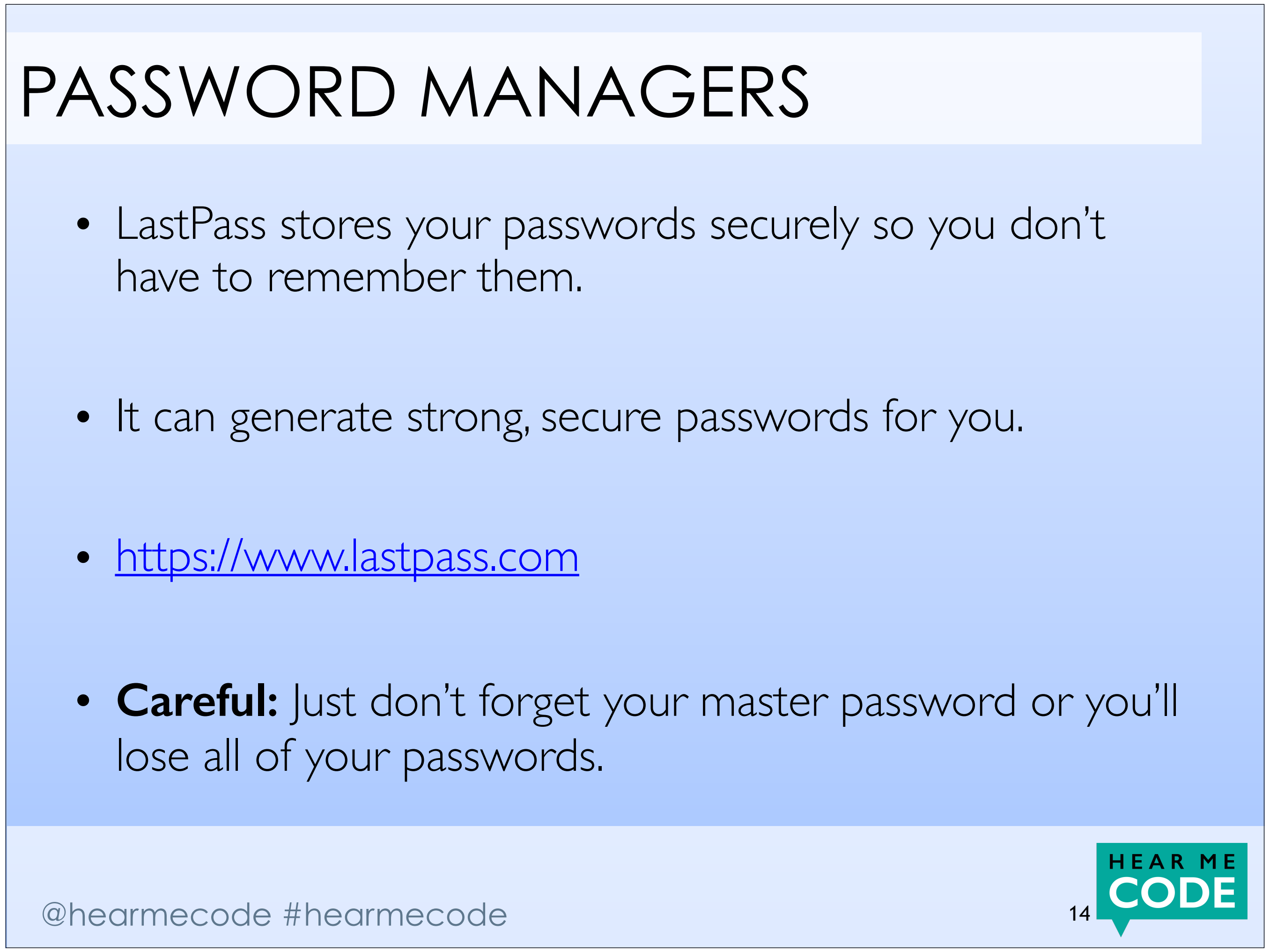


COMMON (BAD) PASSWORDS

Don’t use these in your passwords!

1. Birthdays, especially of family, children, partners
2. “password” or “secret” or “qwerty”
3. The same thing repeated over and over
4. Names of your pets or children
5. Anything that could be guessed from your Facebook

These are very commonly used in passwords — if you have these in your passwords, you’ll want to change them!

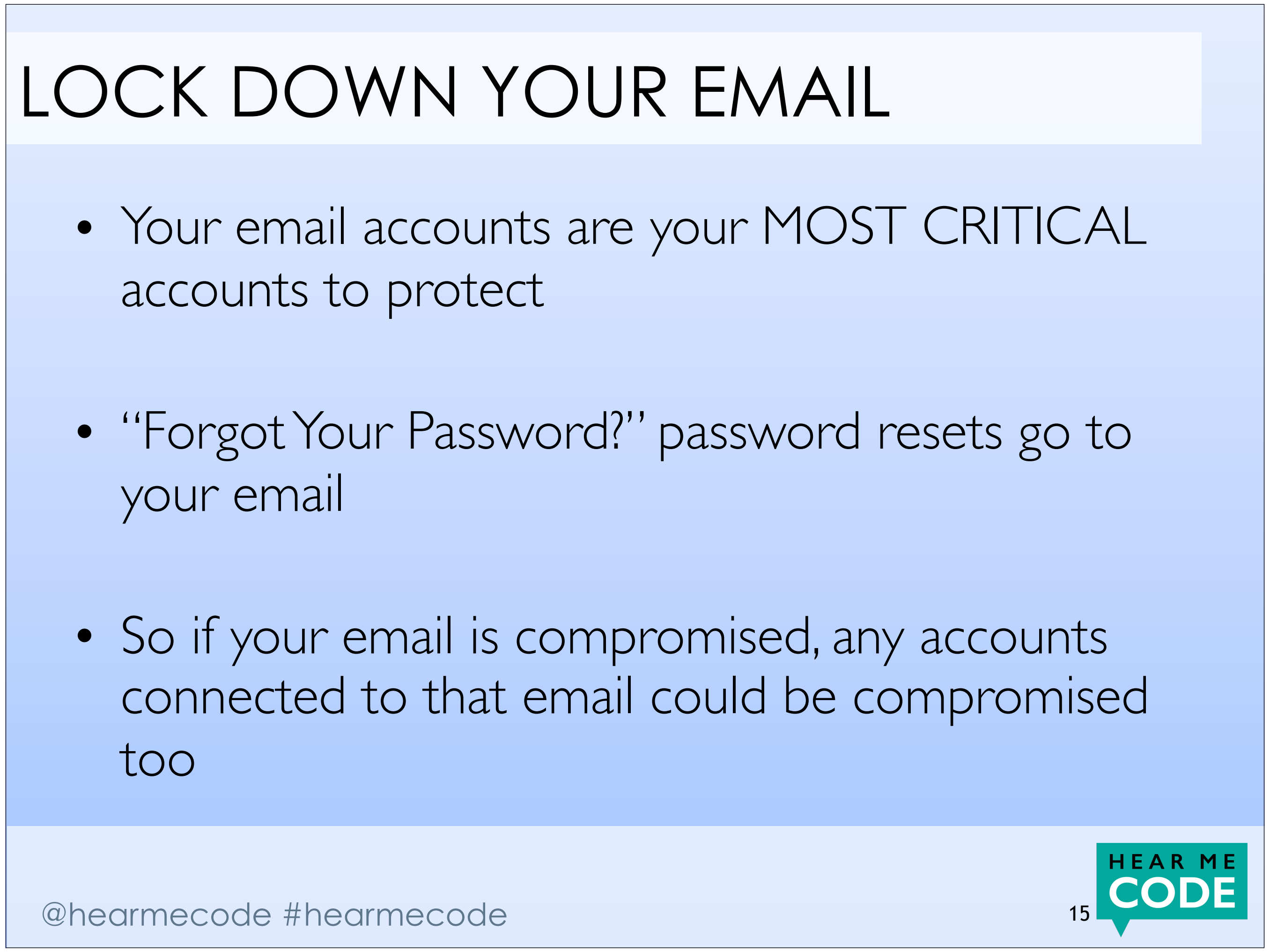


PASSWORD MANAGERS

- LastPass stores your passwords securely so you don't have to remember them.
- It can generate strong, secure passwords for you.
- https://www.lastpass.com
- **Careful:** Just don't forget your master password or you'll lose all of your passwords.

There are many password managers out there, but I like and use LastPass.

It's free for personal use! One of the best features of LastPass is that it can generate long, secure passwords for you.

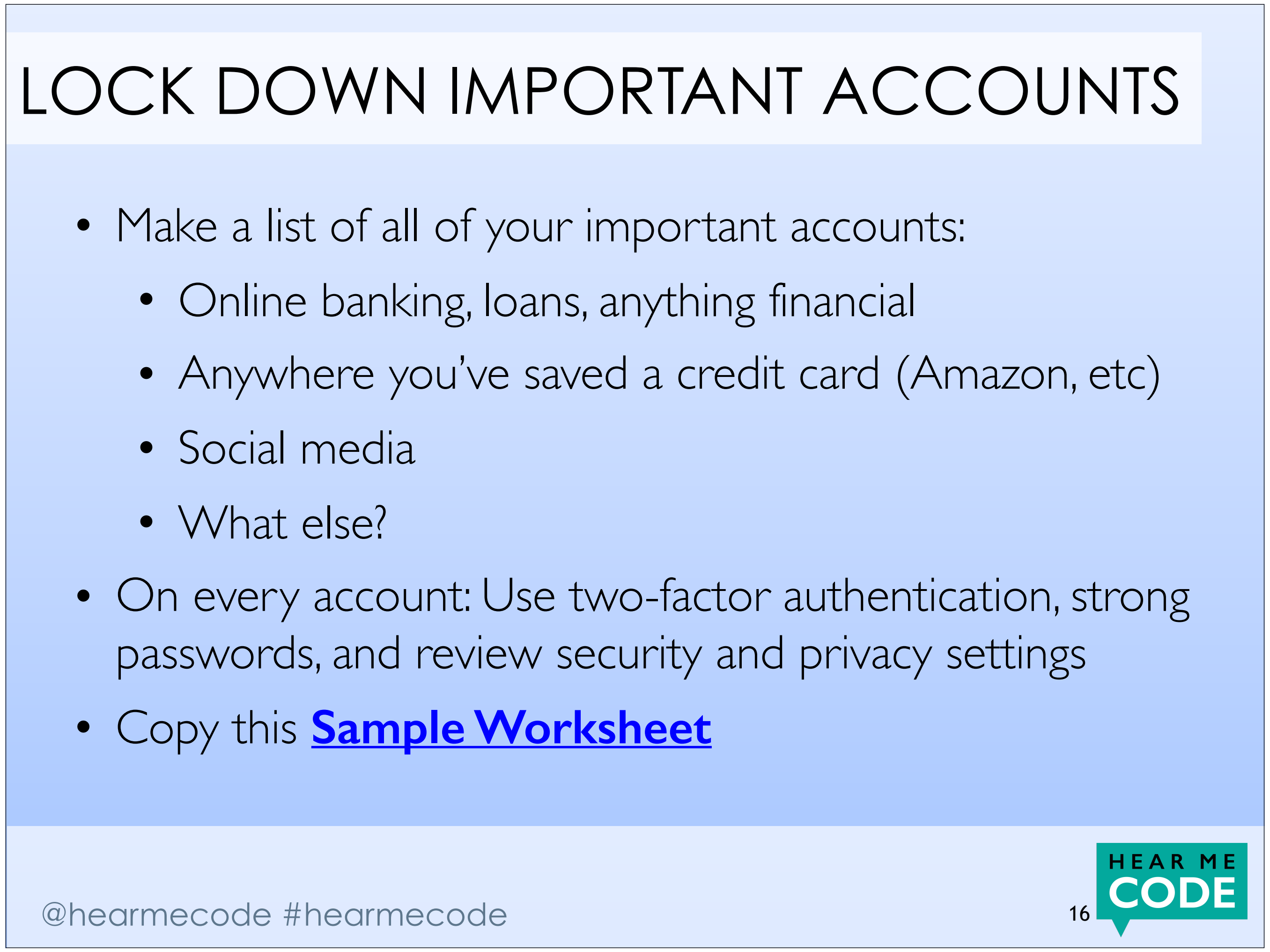


LOCK DOWN YOUR EMAIL

- Your email accounts are your MOST CRITICAL accounts to protect
- "Forgot Your Password?" password resets go to your email
- So if your email is compromised, any accounts connected to that email could be compromised too

Secure your email accounts first, and use two-factor authentication and strong passwords.

Google has a security check with many settings to give you peace of mind in addition to two-factor authentication, so be sure to walk through each step carefully.



LOCK DOWN IMPORTANT ACCOUNTS

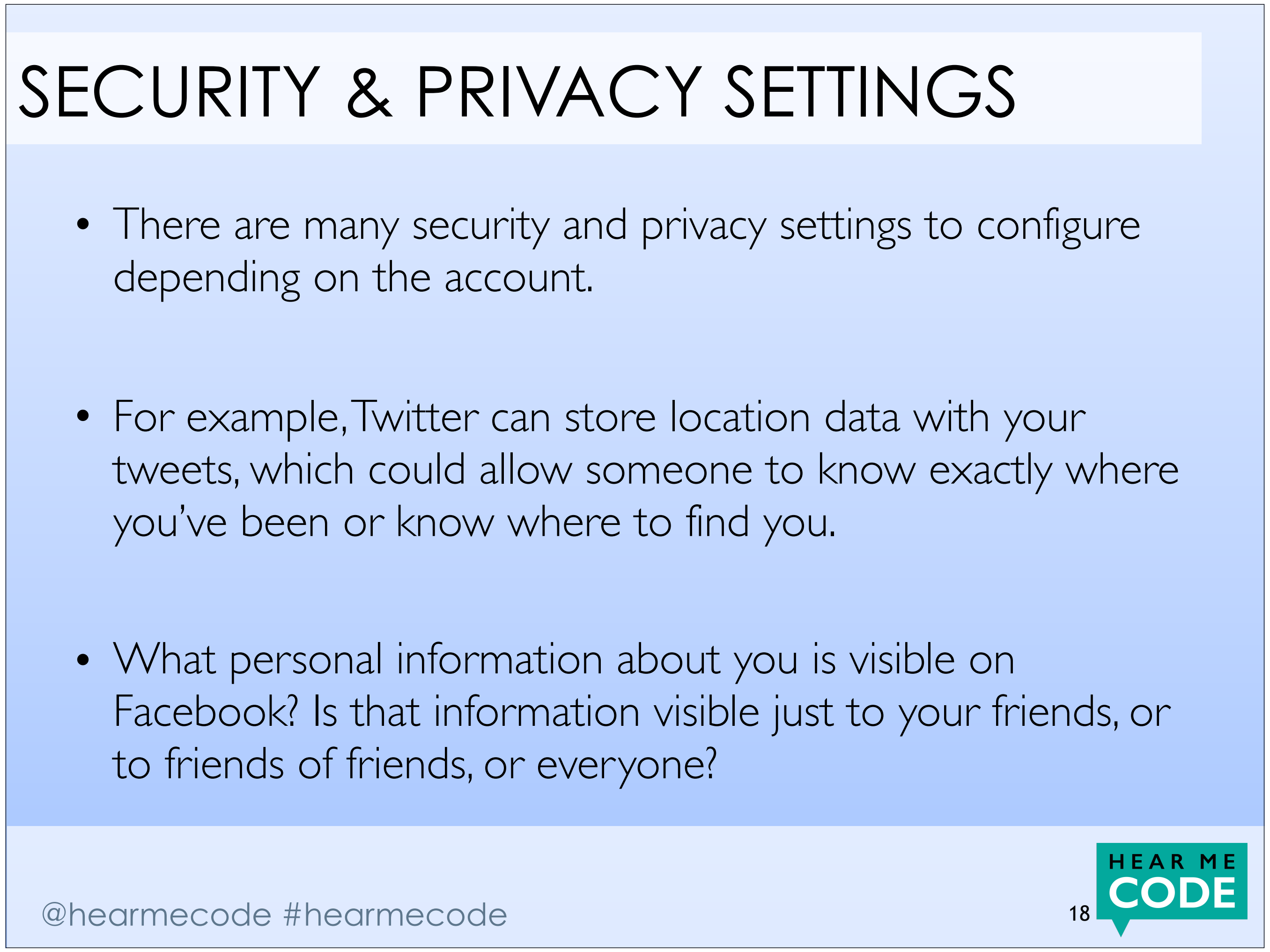
- Make a list of all of your important accounts:
  - Online banking, loans, anything financial
  - Anywhere you've saved a credit card (Amazon, etc)
  - Social media
  - What else?
- On every account: Use two-factor authentication, strong passwords, and review security and privacy settings
- Copy this **Sample Worksheet**

(This doesn't list every type of account because it's important to have folks think about what their specific types of accounts are)

You'll want to brainstorm every online account that you have and make a list. Keep a spreadsheet if it helps you, and track whether you're using a strong password, whether you have two-factor authentication enabled, and whether you've reviewed the security and privacy settings.

One thing to keep in mind: many accounts offer two-factor authentication but not all will.

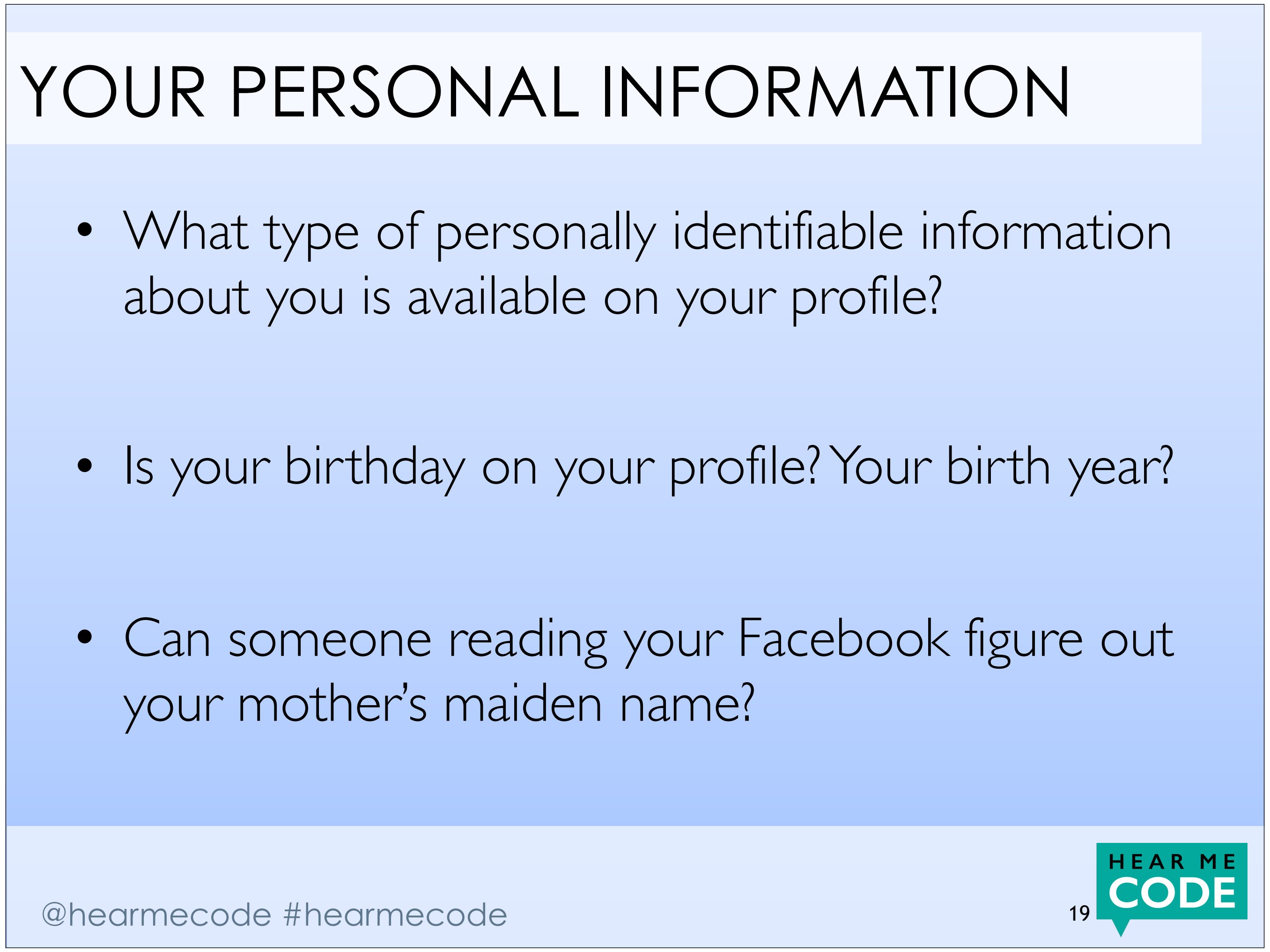
PRIVACY SETTINGS AND YOUR PERSONAL INFO



SECURITY & PRIVACY SETTINGS

- There are many security and privacy settings to configure depending on the account.
- For example, Twitter can store location data with your tweets, which could allow someone to know exactly where you've been or know where to find you.
- What personal information about you is visible on Facebook? Is that information visible just to your friends, or to friends of friends, or everyone?

Every account will have its own security and privacy settings to learn and review, and you may need to review them periodically as new features are added. Facebook is notorious for adding new features and changing existing ones.



YOUR PERSONAL INFORMATION

- What type of personally identifiable information about you is available on your profile?
- Is your birthday on your profile? Your birth year?
- Can someone reading your Facebook figure out your mother's maiden name?

Your birthday and your mother's maiden name are often used as security questions to verify your identity when talking to your bank, for example. Think about the worst case scenarios here - and be very careful about the things you share online for everyone to read.

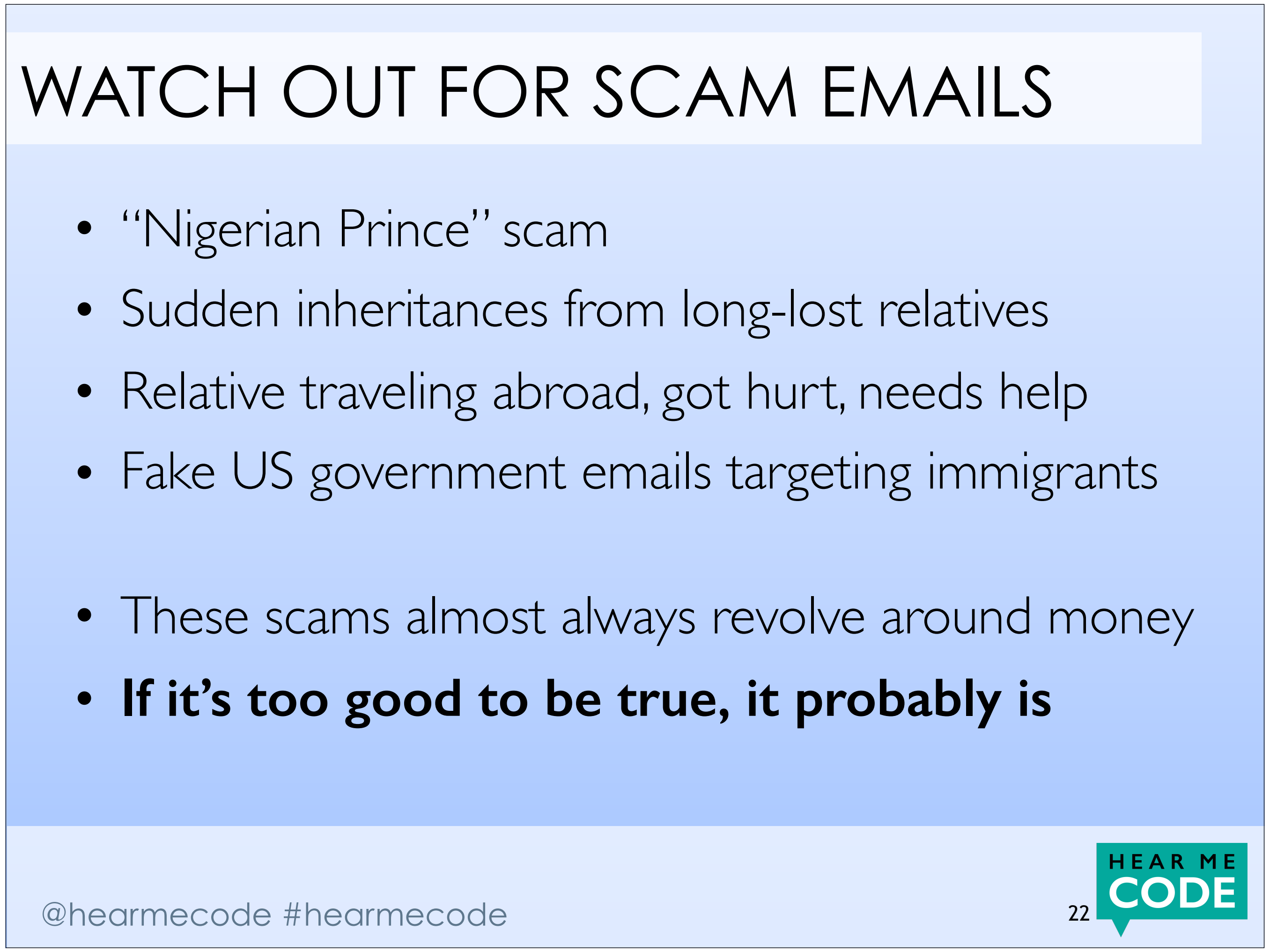
RECOGNIZING & AVOIDING FRAUDULENT EMAILS

TRICKING YOU IS EASIER THAN HACKING

- Why hack into a system if they can trick you into handing over the keys?

- **Nobody legitimate will ever ask you for your password.**

- A common trick is someone "from IT" calling to tell you they need to fix a "problem with your account"



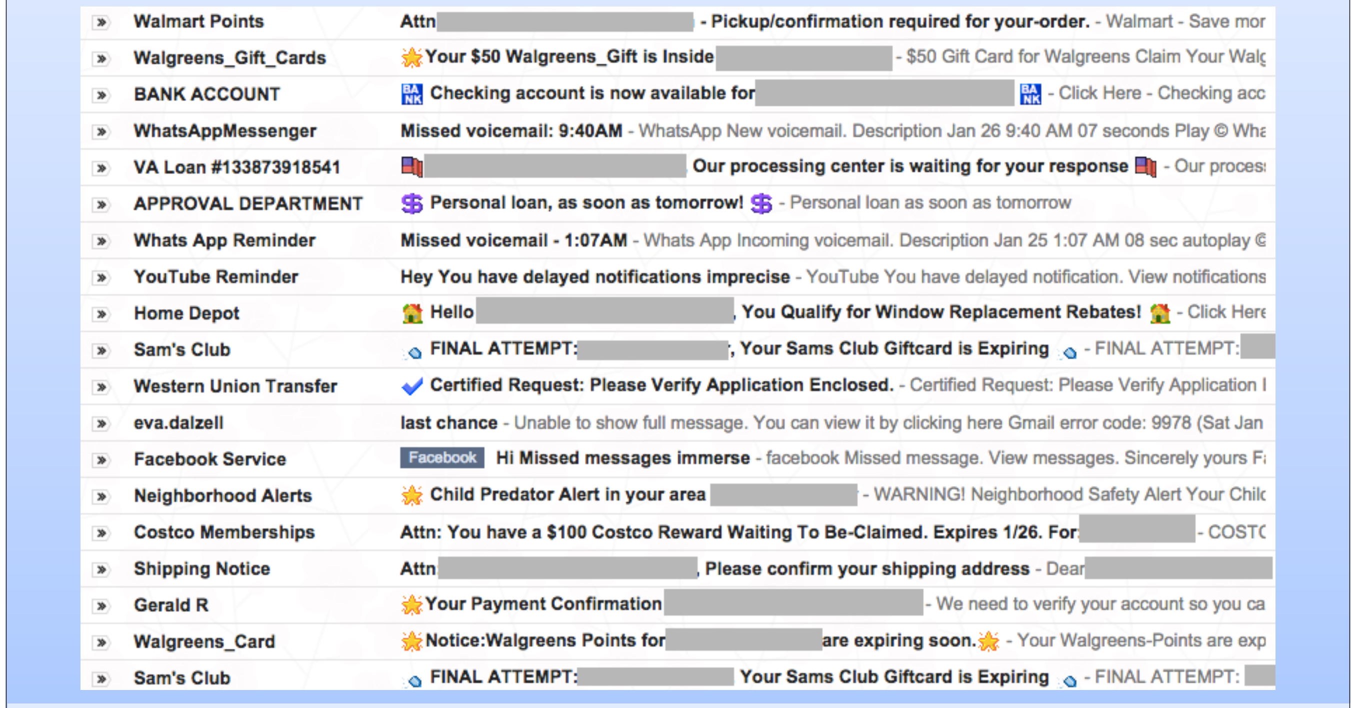
WATCH OUT FOR SCAM EMAILS

- "Nigerian Prince" scam
- Sudden inheritances from long-lost relatives
- Relative traveling abroad, got hurt, needs help
- Fake US government emails targeting immigrants

- These scams almost always revolve around money
- **If it's too good to be true, it probably is**

1) Just give me your bank account number and I will route the money to you!
2) You just need to pay inheritance tax on your newfound riches first!
3) The details are often spotty or missing, but the sense of urgency or missed opportunity can get you
4) Beware of emails that claim they are from the US government, promising an expedited green card, or saying there is a problem with your immigration status and you need to send money to fix it

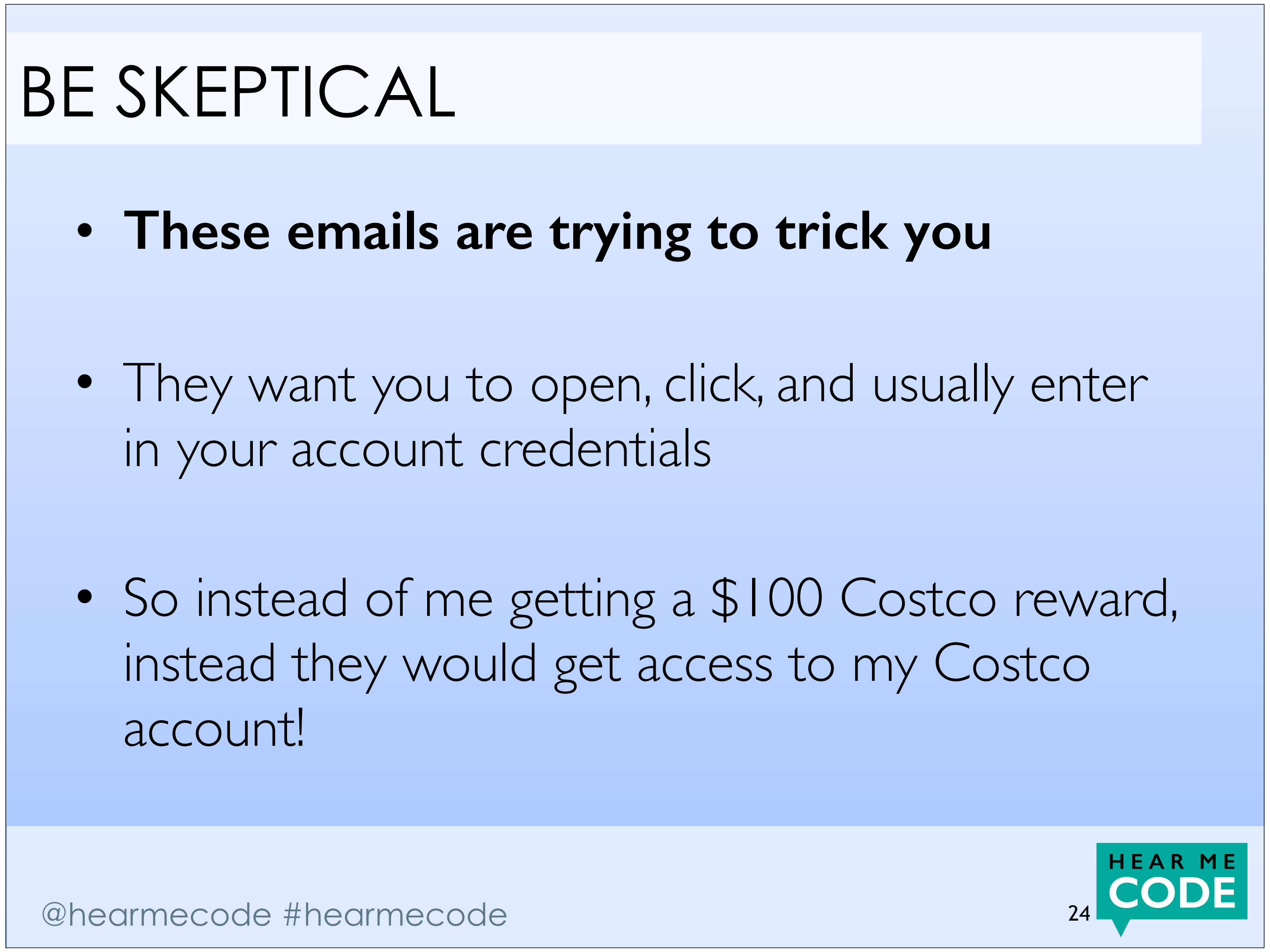
BE SKEPTICAL



Walmart Points	Attn [redacted] - Pickup/confirmation required for your-order. - Walmart - Save mor
Walgreens_Gift_Cards	★Your $50 Walgreens_Gift is Inside [redacted] - $50 Gift Card for Walgreens Claim Your Walg
BANK ACCOUNT	Checking account is now available for [redacted] - Click Here - Checking acc
WhatsAppMessenger	Missed voicemail: 9:40AM - WhatsApp New voicemail. Description Jan 26 9:40 AM 07 seconds Play © Wha
VA Loan #133873918541	[redacted] Our processing center is waiting for your response - Our proces
APPROVAL DEPARTMENT	$ Personal loan, as soon as tomorrow! $ - Personal loan as soon as tomorrow
Whats App Reminder	Missed voicemail - 1:07AM - Whats App Incoming voicemail. Description Jan 25 1:07 AM 08 sec autoplay ©
YouTube Reminder	Hey You have delayed notifications imprecise - YouTube You have delayed notification. View notifications
Home Depot	Hello [redacted], You Qualify for Window Replacement Rebates! - Click Here
Sam's Club	FINAL ATTEMPT: [redacted], Your Sams Club Giftcard is Expiring - FINAL ATTEMPT: [redacted]
Western Union Transfer	✓ Certified Request: Please Verify Application Enclosed. - Certified Request: Please Verify Application I
eva.dalzell	last chance - Unable to show full message. You can view it by clicking here Gmail error code: 9978 (Sat Jan
Facebook Service	Facebook Hi Missed messages immerse - facebook Missed message. View messages. Sincerely yours F
Neighborhood Alerts	★ Child Predator Alert in your area [redacted] - WARNING! Neighborhood Safety Alert Your Chil
Costco Memberships	Attn: You have a $100 Costco Reward Waiting To Be-Claimed. Expires 1/26. For [redacted] - COSTC
Shipping Notice	Attn [redacted], Please confirm your shipping address - Dear [redacted]
Gerald R	★Your Payment Confirmation [redacted] - We need to verify your account so you ca
Walgreens_Card	★Notice:Walgreens Points for [redacted] are expiring soon.★ - Your Walgreens-Points are exp
Sam's Club	FINAL ATTEMPT: [redacted] Your Sams Club Giftcard is Expiring - FINAL ATTEMPT: [redacted]

Here is a sampling of fraudulent / phishing emails I've received. Notice how they're all trying to grab my attention and get me to open and click. I have a gift card to claim, a missed voicemail at 1:07 am, a response on a loan, a child predator alert. There's a lot going on here.

These emails are trying to trick you - look at how many of them employ a sense of urgency, or missed opportunity, or make you curious, or appeal to fear or authority.



BE SKEPTICAL

- **These emails are trying to trick you**
- They want you to open, click, and usually enter in your account credentials
- So instead of me getting a $100 Costco reward, instead they would get access to my Costco account!

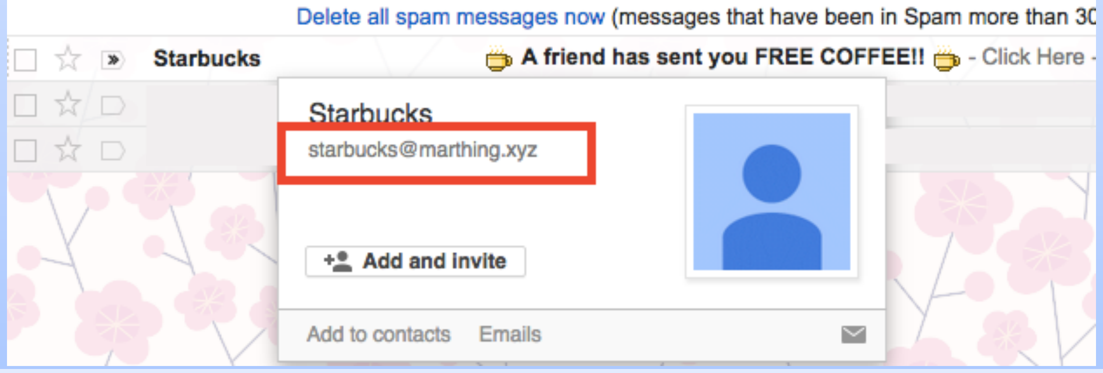
So let’s say I opened up the email from the previous screen that promised a $100 Costco reward that I needed to claim. If I opened the email, clicked through, and logged into my account, I would be giving away my password to the hackers and they could get into my account.

BE SKEPTICAL

- **These emails are trying to trick you**
- Not all fraudulent emails will be so obvious!
- If you can tell it's a fraudulent email without opening, **delete it without opening**!

VERIFY THE SENDER

- Verify the sender by hovering over the sender's name.
- If this were legit, it should come from starbucks.com, not marthing.xyz



Delete all spam messages now (messages that have been in Spam more than 30

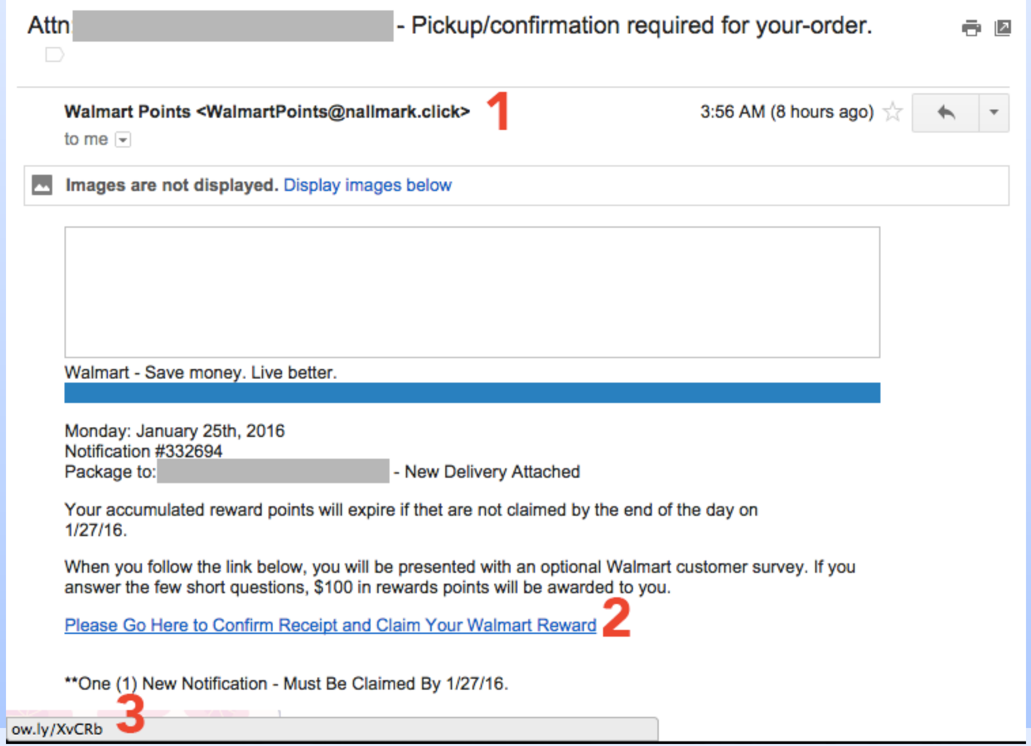
Starbucks — A friend has sent you FREE COFFEE!! - Click Here -

Starbucks
starbucks@marthing.xyz

@hearmecode #hearmecode

Keep in mind that fraudulent emails will often use slight misspellings or spellings that are just a letter off that may look "close enough" if you're not reading closely, going too quickly, or have impaired vision.

VERIFY THE LINK



Attn [redacted] - Pickup/confirmation required for your-order.

Walmart Points <WalmartPoints@nallmark.click> 1
to me
3:56 AM (8 hours ago)

Images are not displayed. Display images below

Walmart - Save money. Live better.

Monday: January 25th, 2016
Notification #332694
Package to: [redacted] - New Delivery Attached

Your accumulated reward points will expire if thet are not claimed by the end of the day on 1/27/16.

When you follow the link below, you will be presented with an optional Walmart customer survey. If you answer the few short questions, $100 in rewards points will be awarded to you.

Please Go Here to Confirm Receipt and Claim Your Walmart Reward 2

**One (1) New Notification - Must Be Claimed By 1/27/16.

ow.ly/XvCRb 3

If we accidentally opened a fraudulent email, we can still figure out that it's a fake.

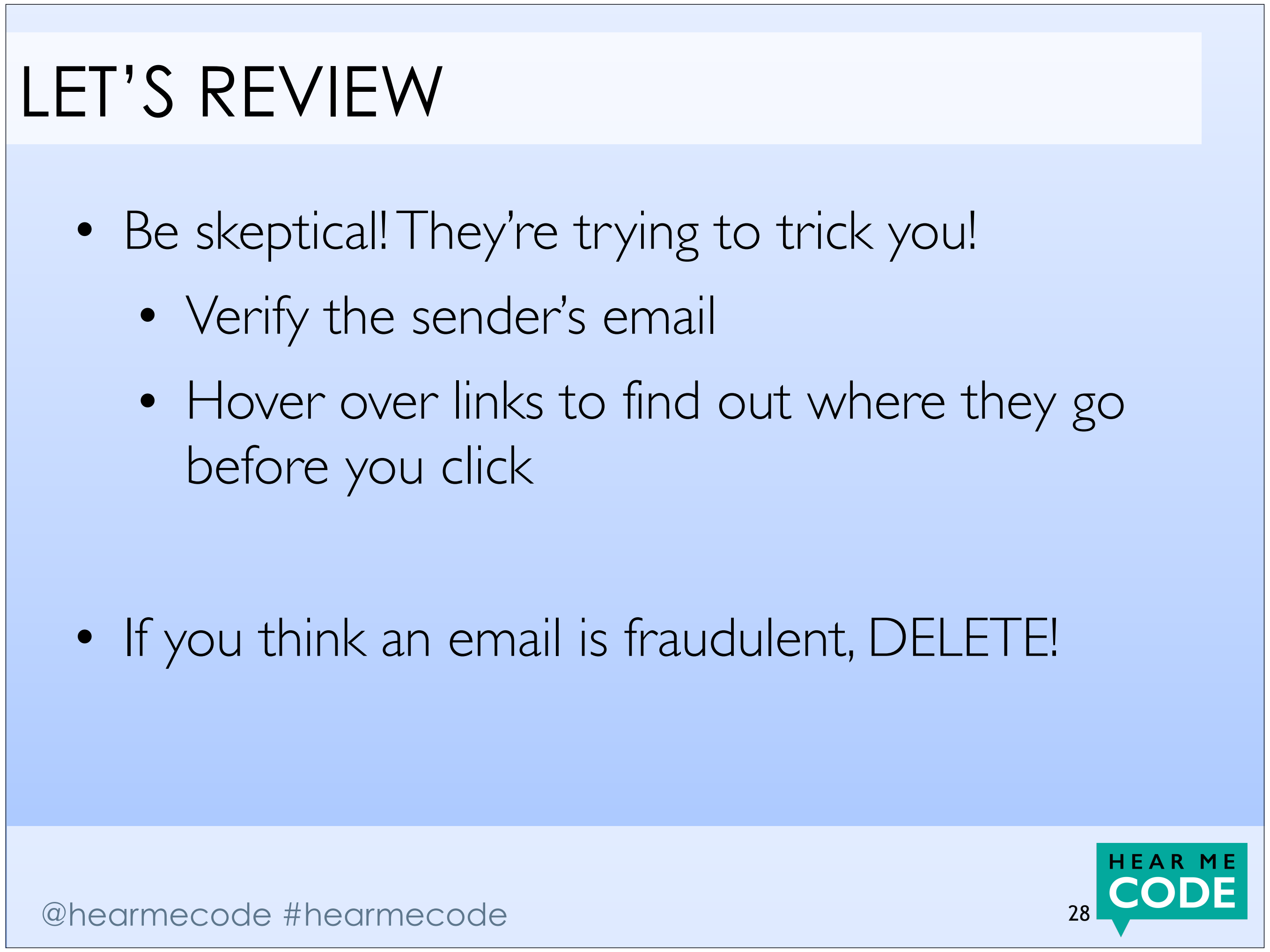
In #1 we see that the return address is nallmark.click, not walmart.com as we might expect if this were legit. Remember that they'll often rely on close misspellings.

If we hover over the link shown in #2, the status bar at the bottom of our screen (#3) will show that link that it would take us to, BEFORE we would actually go there. Get in the habit of hovering over links to see where they go before clicking.

In #3 we see that this email has used a link shortener to obfuscate where the link would actually go. If this link were legit, I would expect it to go to walmart.com*

* One caveat is sometimes legitimate email marketers will use long, confusing links that are difficult to figure out exactly where they go. In that case, make sure you trust that email before you click.

Let's say I wasn't sure if I actually did have a Walmart reward waiting to be redeemed. Instead of clicking the link in this email, a better solution would be going to the Walmart website directly and checking my account there.

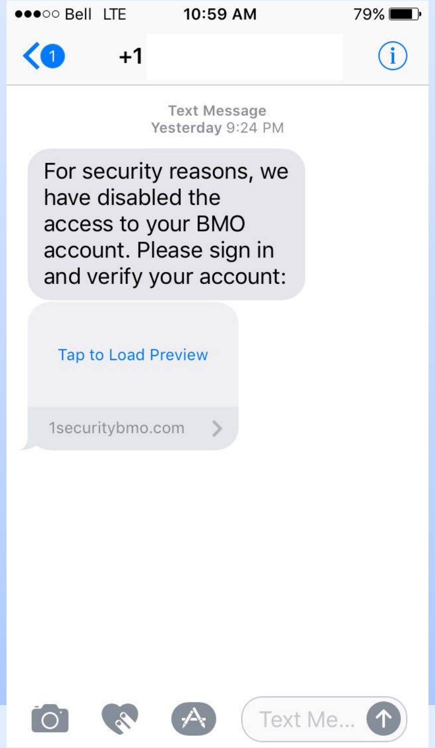


LET'S REVIEW

- Be skeptical! They're trying to trick you!
  - Verify the sender's email
  - Hover over links to find out where they go before you click
- If you think an email is fraudulent, DELETE!

Keep in mind that if you're checking your email on your phone, it's very difficult to verify the sender, and you can't really hover over the link to see where it's going first. So use extra caution when checking email on your phone, and verify when you're on your computer.

WATCH OUT FOR PHISHING TEXT MESSAGES, TOO

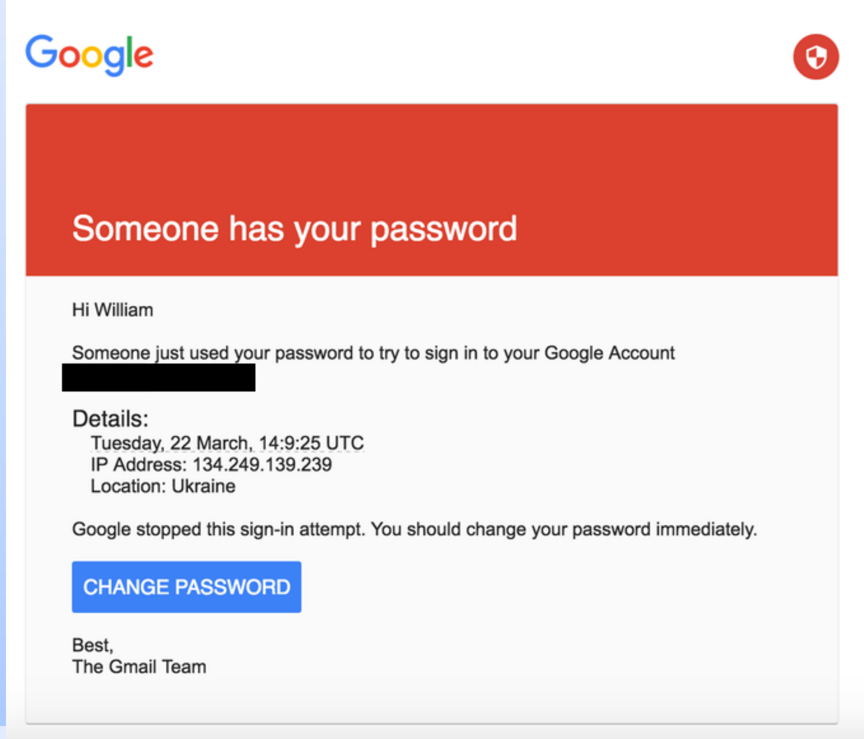


For security reasons, we have disabled the access to your BMO account. Please sign in and verify your account:

Here is an example of a phishing text message - a text from an unrecognized number, asking you to sign in to “verify” your account, a link to click on and open. This is not a legitimate way of verifying any account.

Instead of clicking the link here - you could go to your account’s website directly.

THIS EMAIL LOOKS URGENT …



Someone has your password

Hi William

Someone just used your password to try to sign in to your Google Account
[redacted]

Details:
Tuesday, 22 March, 14:9:25 UTC
IP Address: 134.249.139.239
Location: Ukraine

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

Best,
The Gmail Team

This email looks like I need to change my password right away!

Someone just used my password to sign into my Google Account!

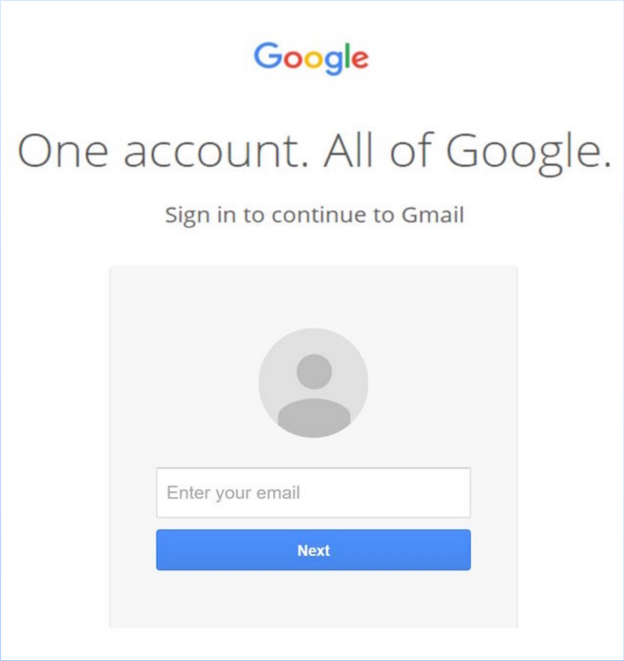
What do I do?

1) Verify the sender’s address.

2) Verify the link the “Change Password” button would go to.

This was the exact email that was sent to staff at the DNC - and because someone clicked and entered in their password, hackers were able to gain access to their whole email account.

… BUT BE CAREFUL



Google

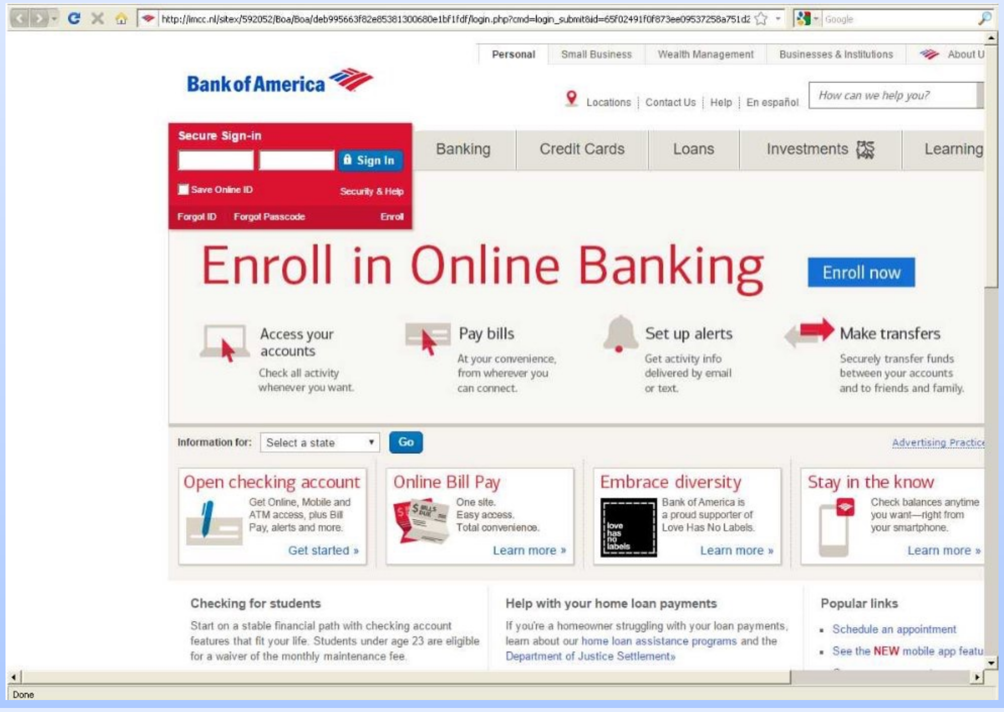
One account. All of Google.

Sign in to continue to Gmail

And if you clicked through, it would look just like Google’s page. You probably wouldn’t be able to tell. Think of all of the sensitive information in your email: everyone you’ve ever communicated with, thinking your conversations were private. Addresses, phone numbers, all of your contacts, where you are, where you’ve been, what you’ve bought, everything.

RECOGNIZING & AVOIDING FRAUDULENT WEBSITES

FRAUDULENT SITES LOOK VERY REAL



http://imcc.nl/sitex/592052/Boa/Boa/deb995663f82e85381300680e1bf1fdf/login.php?cmd=login_submit&id=65f02491f0f873ee09537258a751d2

Enroll in Online Banking

Access your accounts
Check all activity whenever you want.

Pay bills
At your convenience, from wherever you can connect.

Set up alerts
Get activity info delivered by email or text.

Make transfers
Securely transfer funds between your accounts and to friends and family.

Open checking account
Get Online, Mobile and ATM access, plus Bill Pay, alerts and more.

Online Bill Pay
One site.
Easy access.
Total convenience.

Embrace diversity
Bank of America is a proud supporter of Love Has No Labels.

Stay in the know
Check balances anytime you want—right from your smartphone.

Checking for students
Start on a stable financial path with checking account features that fit your life. Students under age 23 are eligible for a waiver of the monthly maintenance fee.

Help with your home loan payments
If you're a homeowner struggling with your loan payments, learn about our home loan assistance programs and the Department of Justice Settlement»

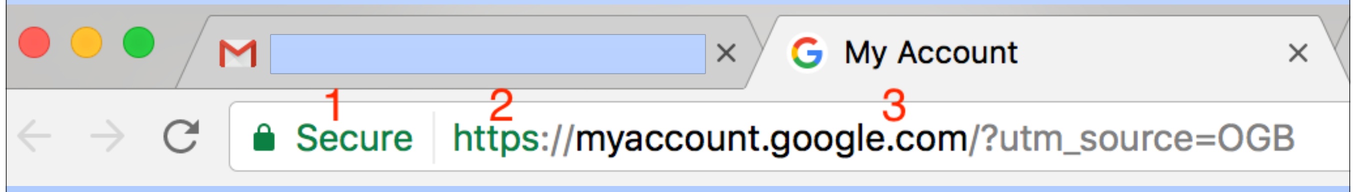
Popular links
- Schedule an appointment
- See the NEW mobile app featu

This is a fraudulent site, but looks just like the Bank of America website.

If I received a fraudulent email, and it got me to click, and I put in my login credentials, I'd be giving away access to my bank account. This is a fraudulent site, and you can tell by the URL.

SO HOW TO VERIFY A URL?

- 1) The padlock tells me the **connection** is secure, not necessarily that the site is legit
- 2) The S at the end of http also means the connection is secure, not necessarily that the site is legit



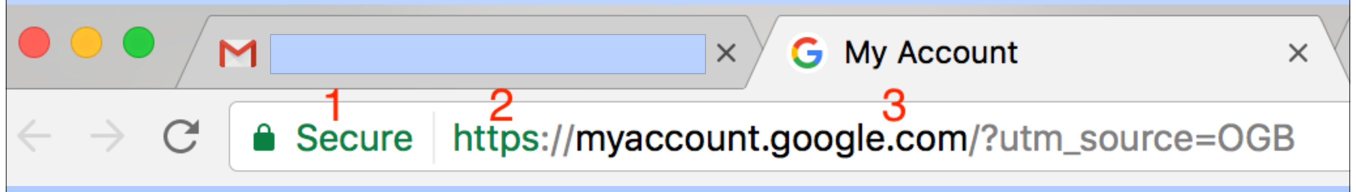
My Account

Secure https://myaccount.google.com/?utm_source=OGB

If there isn't a padlock, it's not a secure connection, even if it says https.

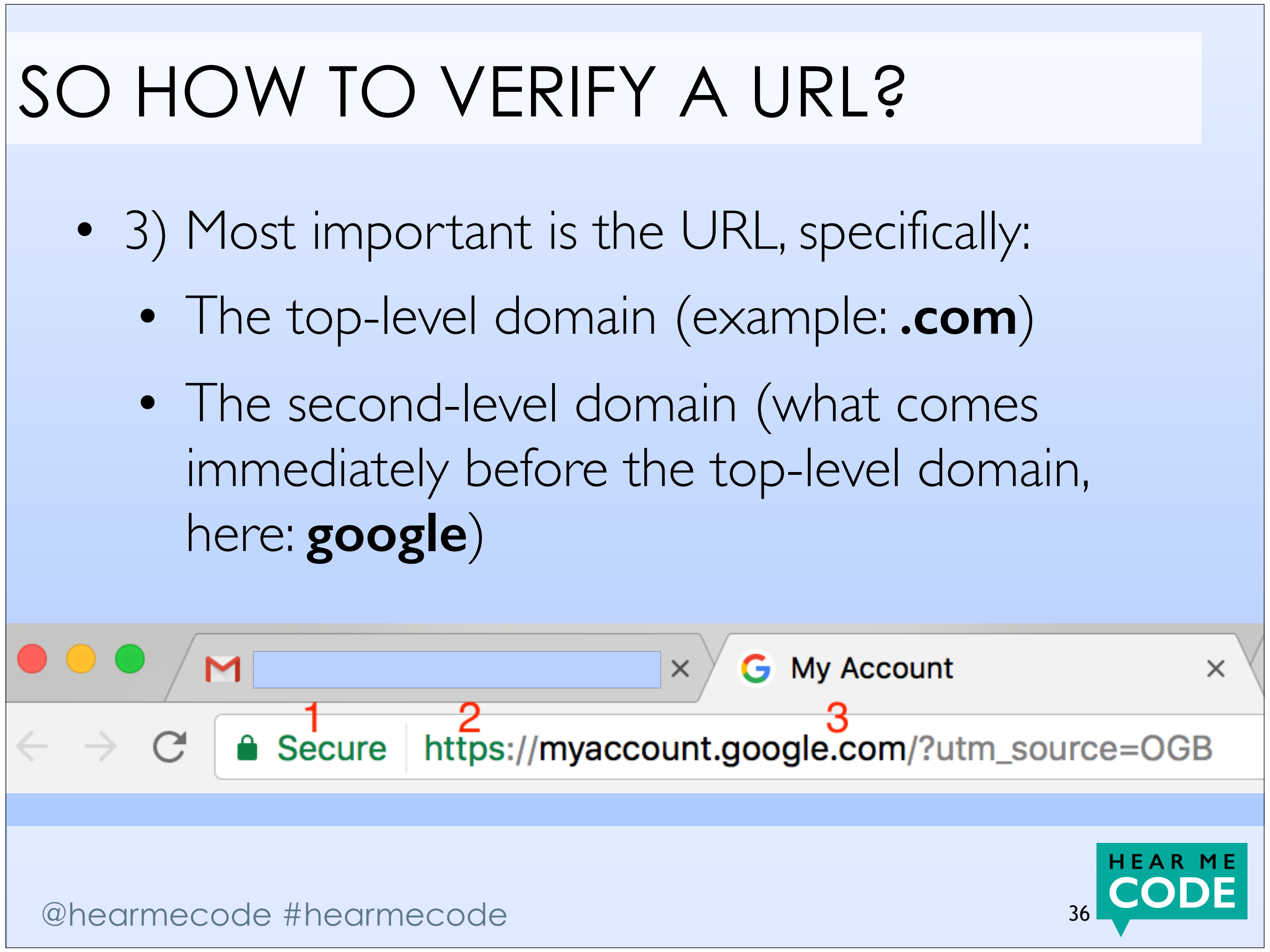
HTTPS ISN'T EVERYWHERE

- Many legitimate sites are not configured to use https for secure connections, and that's okay.
- But if the connection is NOT secure, then entering your username, password, and any sensitive data is NOT recommended.



https://myaccount.google.com/?utm_source=OGB

Without the padlock, it's possible in theory for a hacker to intercept and read the webpage when communicating between your computer and that website.



SO HOW TO VERIFY A URL?

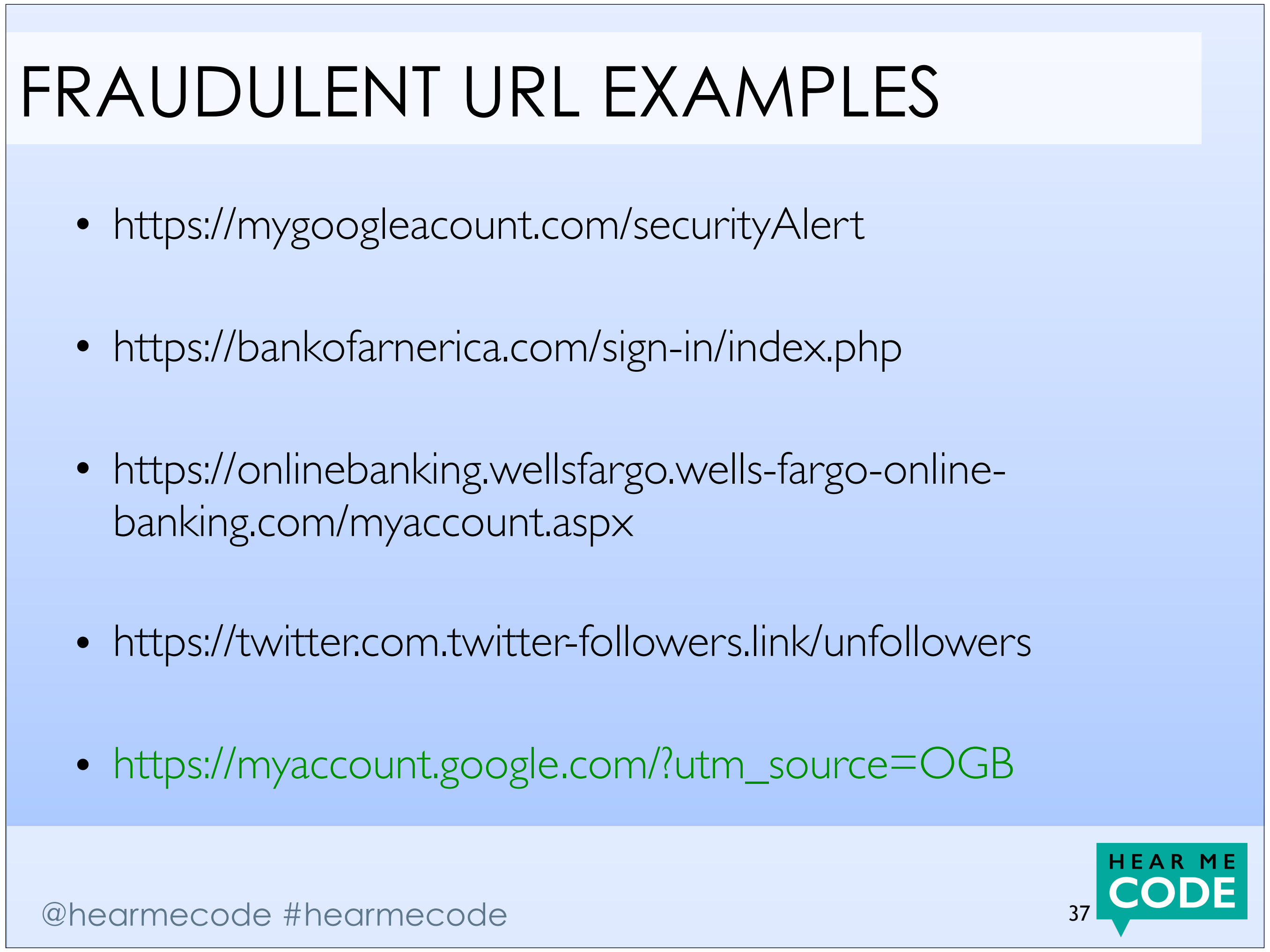
- 3) Most important is the URL, specifically:
  - The top-level domain (example: **.com**)
  - The second-level domain (what comes immediately before the top-level domain, here: **google**)

Secure https://myaccount.google.com/?utm_source=OGB

There's a lot of jargon here but it's important, because this is the most important part of verifying a URL.

What you're going to look for is the **domain,** which appears between the https:// (or http://) and the first slash you see after that. In this example, the full domain is myaccount.google.com. Once you know that full domain, you can figure out the top-level and second-level domains by moving from right to left.

(Spend less time on this slide and more time on the examples.)



FRAUDULENT URL EXAMPLES

- https://mygoogleacount.com/securityAlert
- https://bankofarnerica.com/sign-in/index.php
- https://onlinebanking.wellsfargo.wells-fargo-online-banking.com/myaccount.aspx
- https://twitter.com.twitter-followers.link/unfollowers
- https://myaccount.google.com/?utm_source=OGB

DISCLAIMER: I MADE ALL OF THESE LINKS UP, DON'T VISIT THESE SITES, I DON'T KNOW WHAT IS THERE BUT YOU SHOULD NOT FIND OUT

How do we know each of these is fake? The top-level and second-level domains is not the correct URL in any of these examples.

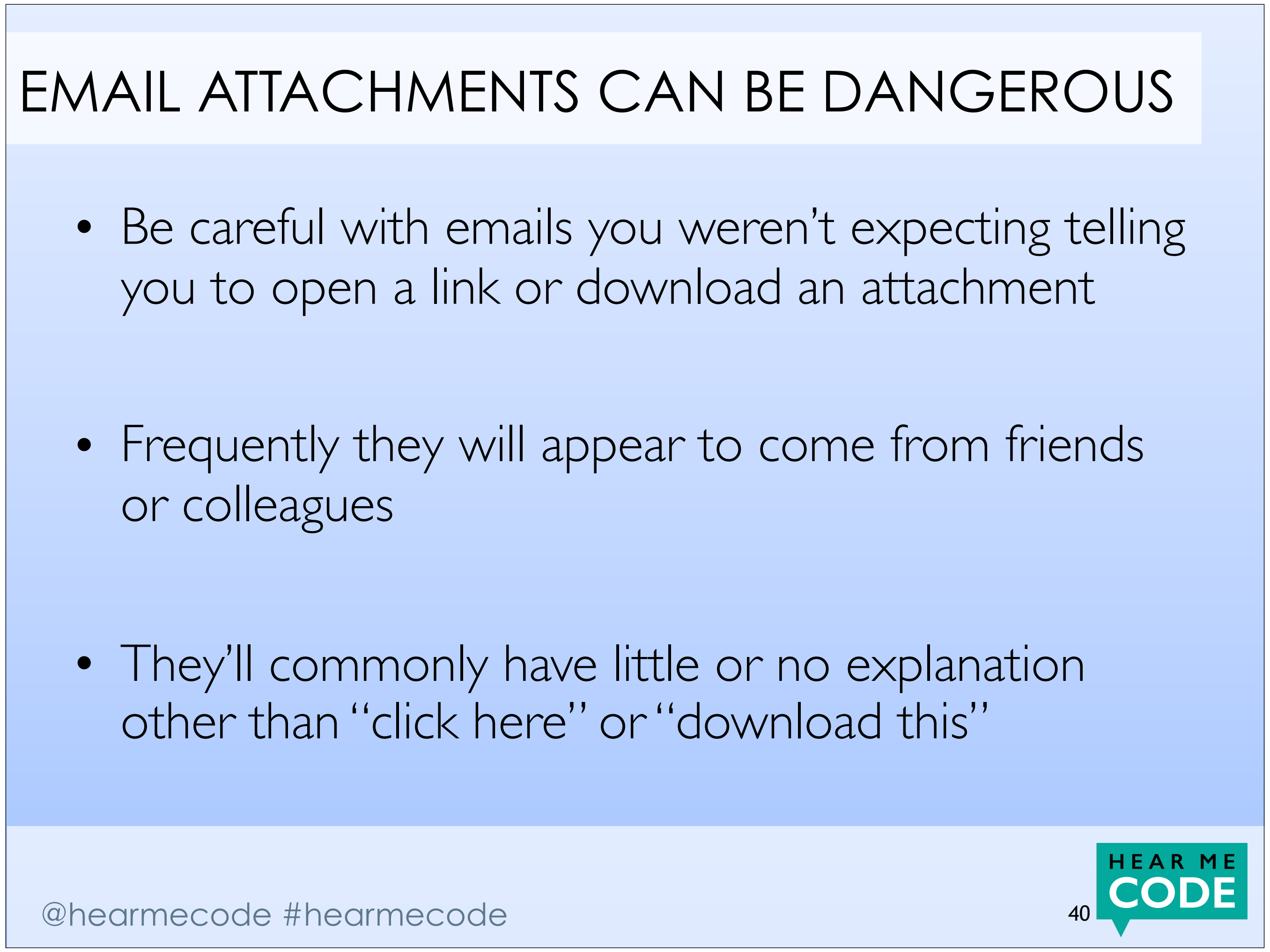
1) Google's URL is google.com, not this, and it's missing a C anyway
2) A lowercase R and N next to each other can often easily be mistaken for an M, especially for those with impaired vision and in certain fonts.
3) Many fake URLs will make the first part of the URL look legit, but that's NOT the important part
4) What's the top-level domain here? What's the second-level domain?
5) The fifth example here is actually a legitimate URL, shown here for contrast. What is the top-level domain here? What is the second-level domain?

RECOGNIZING & AVOIDING MALICIOUS EMAIL ATTACHMENTS

WHAT'S THE DANGER?

- Clicking links in fraudulent emails will often lead to websites designed to steal your account credentials and/or infect your computer

- Downloading malicious attachments will infect your computer with a virus



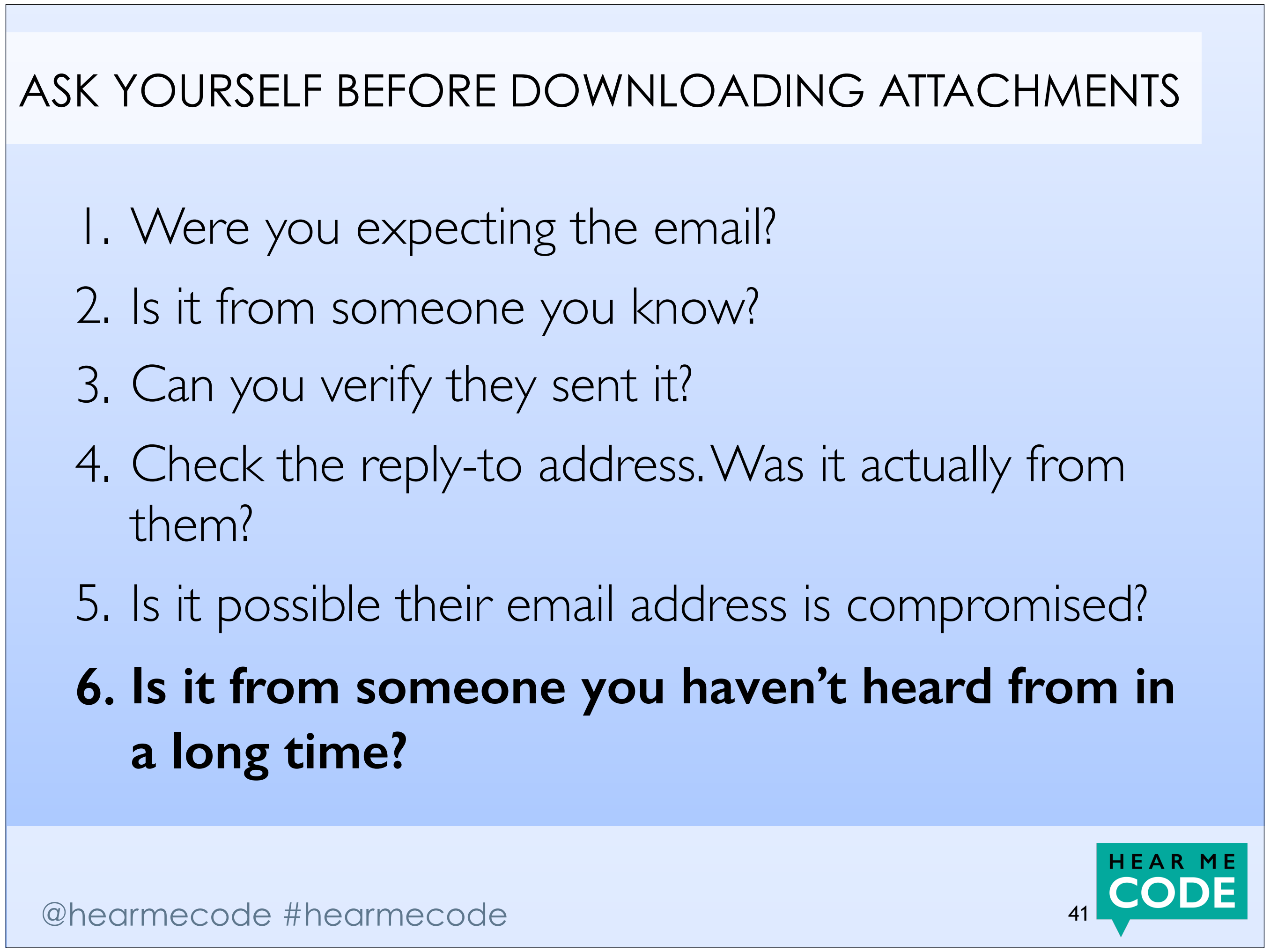
EMAIL ATTACHMENTS CAN BE DANGEROUS

- Be careful with emails you weren't expecting telling you to open a link or download an attachment
- Frequently they will appear to come from friends or colleagues
- They'll commonly have little or no explanation other than "click here" or "download this"

We've talked a lot about email because email is one of the most common ways you'll encounter threats - so far we've seen phishing emails and scam emails.

I've received malicious email attachments from a former colleague whose email account was compromised - they had a virus on their computer and didn't realize they were sending out emails to people in their address book with copies of that virus in attachments.

I hadn't spoken to her in over a year, so when I got an email from her telling me I should open up an attachment that had her "vacation pictures" I knew something was wrong.



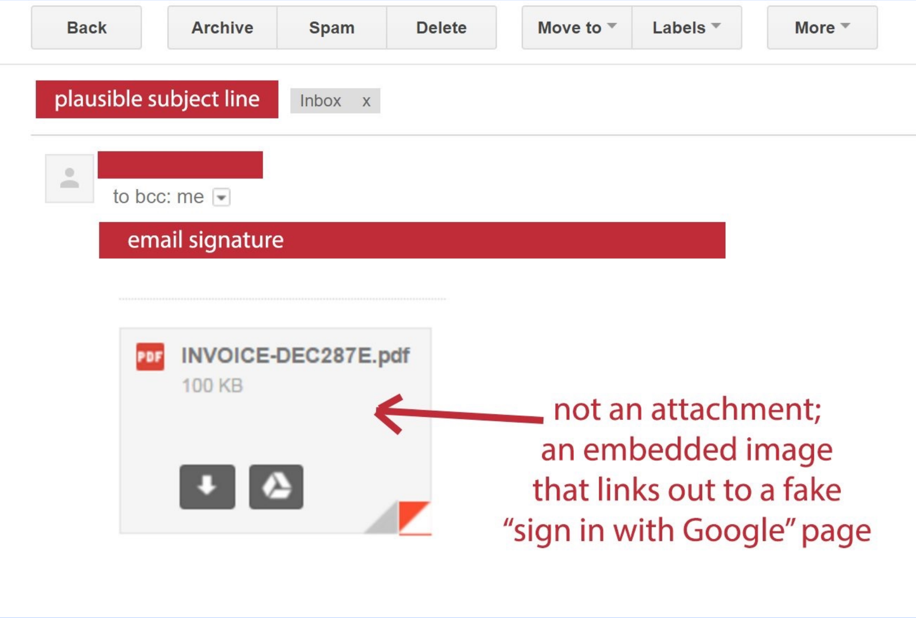
ASK YOURSELF BEFORE DOWNLOADING ATTACHMENTS

1. Were you expecting the email?
2. Is it from someone you know?
3. Can you verify they sent it?
4. Check the reply-to address. Was it actually from them?
5. Is it possible their email address is compromised?
6. **Is it from someone you haven’t heard from in a long time?**

Once an email is compromised, hackers will go through the address book and send to that person’s contacts. They’re relying on you trusting your friend or colleague and opening an attachment from them without thinking about it, without applying the skepticism you should.

Apply the same level of caution when receiving links out of the blue, and verify where the links go before clicking on them!

SOME ATTACHMENTS ARE NOT ATTACHMENTS AT ALL



plausible subject line

Inbox x

[redacted]

to bcc: me

email signature

INVOICE-DEC287E.pdf

100 KB

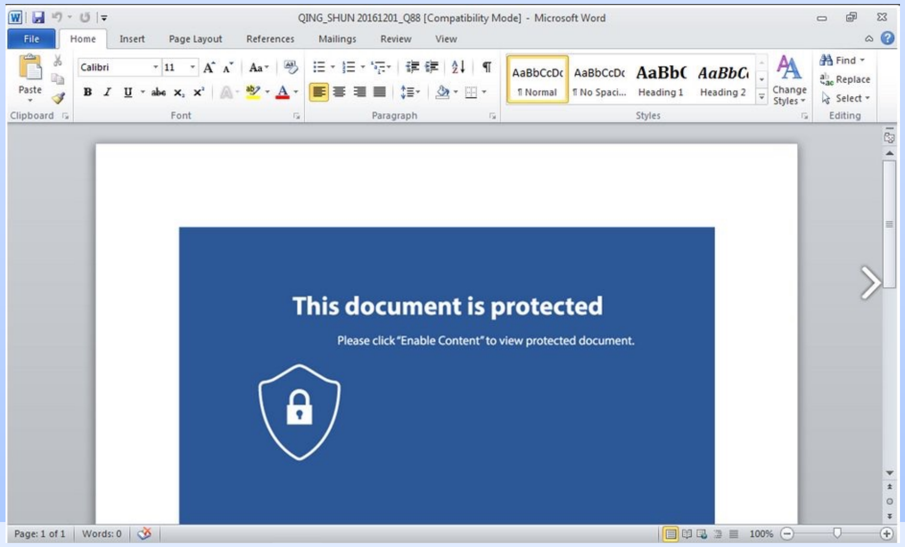
not an attachment; an embedded image that links out to a fake “sign in with Google” page

In Gmail, if this were a legitimate attachment, there would be two buttons - Download and Save to Drive - that you could hover over.

In this fraudulent image, those buttons are faked, and hovering over them would do nothing — that is a big red flag, and a sign that you should not click.

BE CAREFUL WITH OFFICE DOCUMENTS

- Many fraudulent attachments will try to trick you into disabling Office's built-in protections



QING_SHUN 20161201_Q88 [Compatibility Mode] - Microsoft Word

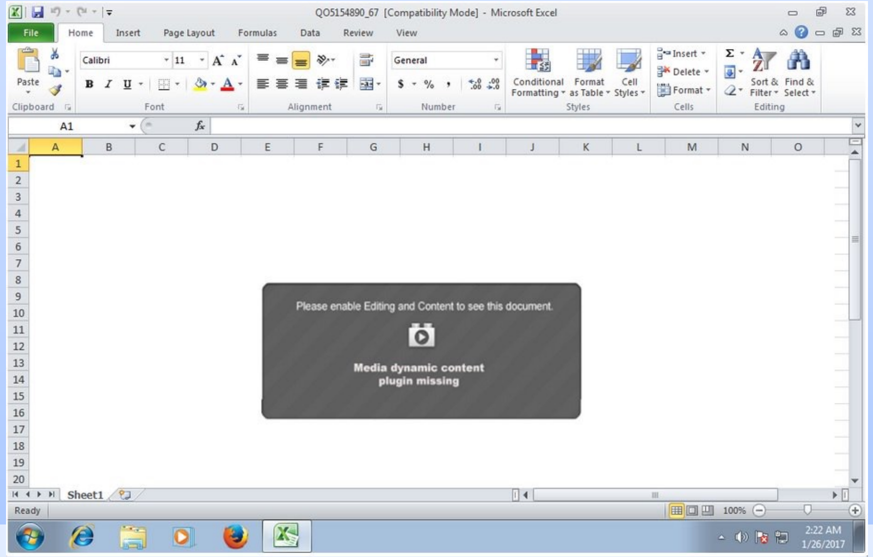
This document is protected

Please click "Enable Content" to view protected document.

There's nothing actually here in this document, but once you follow the instructions, you'll have a virus on your computer. If you see a document like this, close it and delete it — don't follow the instructions.

BE CAREFUL WITH OFFICE DOCUMENTS

- Office documents are the most common type of attachment, and they're safe, right?



QO5154890_67 [Compatibility Mode] - Microsoft Excel

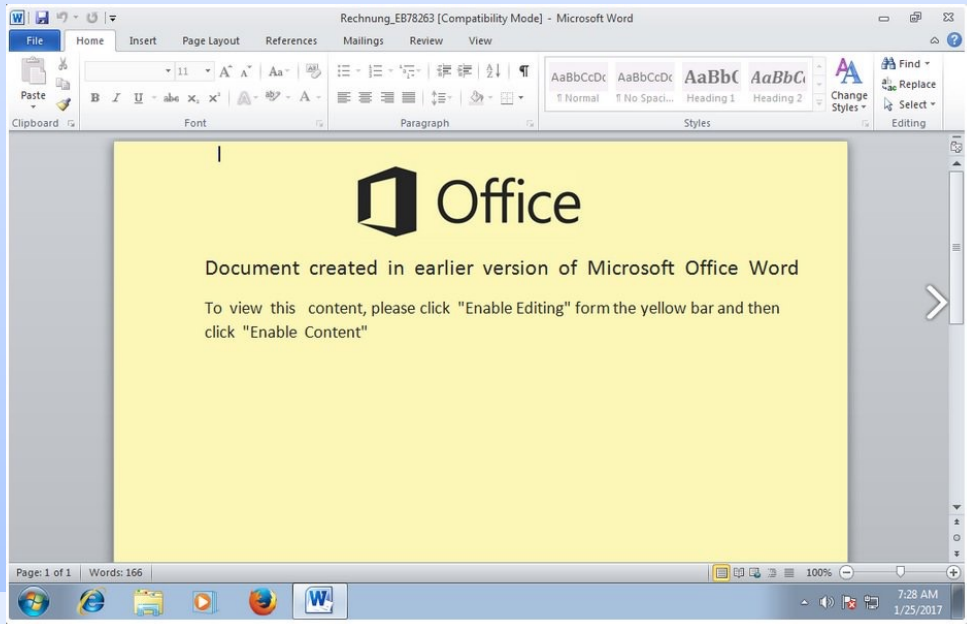
Please enable Editing and Content to see this document.

Media dynamic content plugin missing

This is another version of the same malicious attachment.

BE CAREFUL WITH OFFICE DOCUMENTS

- There are dozens of versions of this trick



Document created in earlier version of Microsoft Office Word

To view this content, please click "Enable Editing" form the yellow bar and then click "Enable Content"

@hearmecode #hearmecode

Yet another version of the same type of malicious attachment. I have so many screenshots of these.

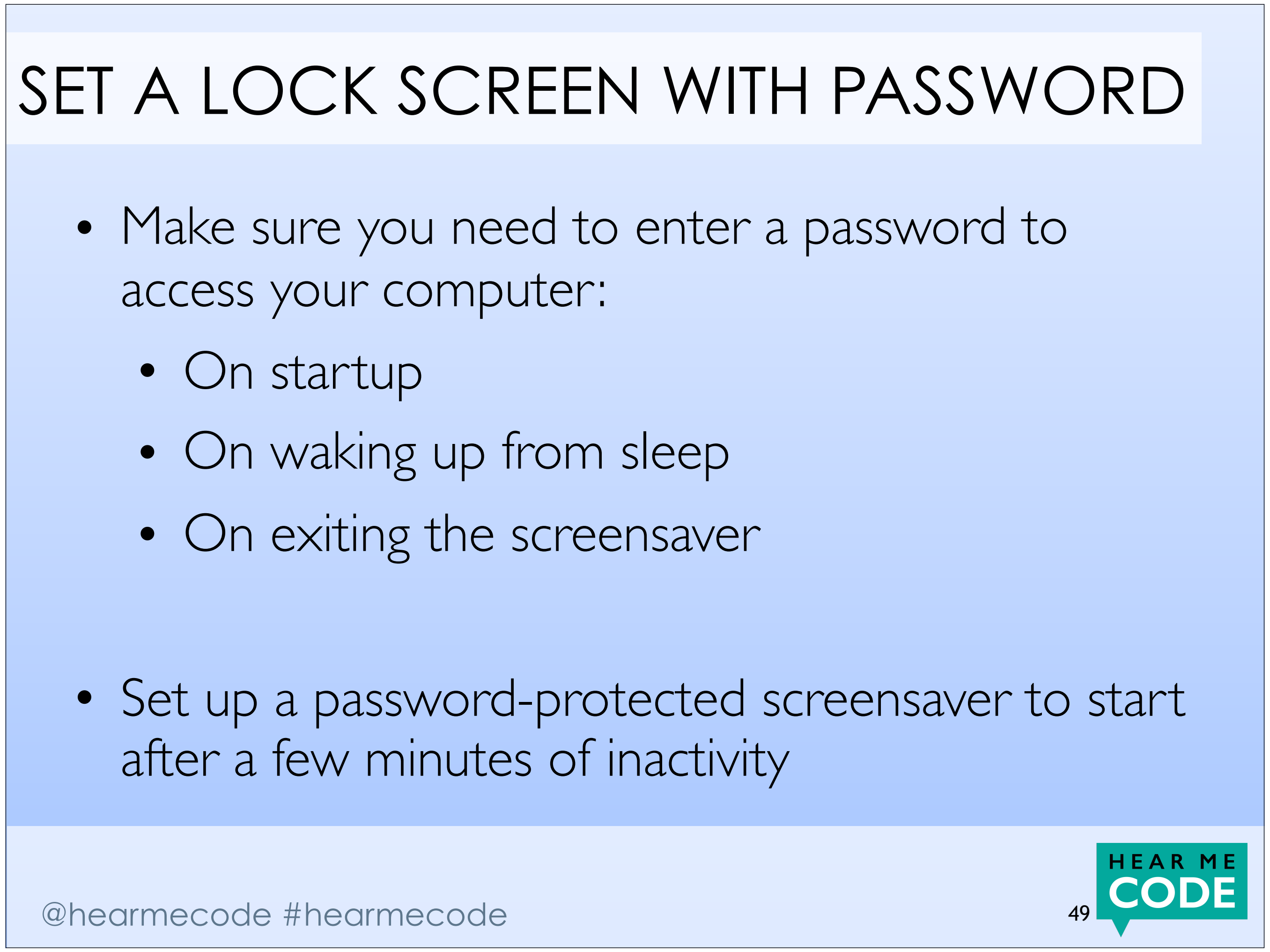
BE CAREFUL WHAT YOU DOWNLOAD

- Don’t download counterfeit software
- Don’t download programs that promise free system scans or PC speed boosts
- Especially if they advertise with pop-up windows or flashing advertisements
- Download software only from trusted websites

AUTOMATIC UPDATES

- **Keep your software up to date**
- It can be annoying to have to restart your computer to install updates, but don't put it off
- Updates often contain critical security updates
- Set up automatic updates to make it easier on yourself

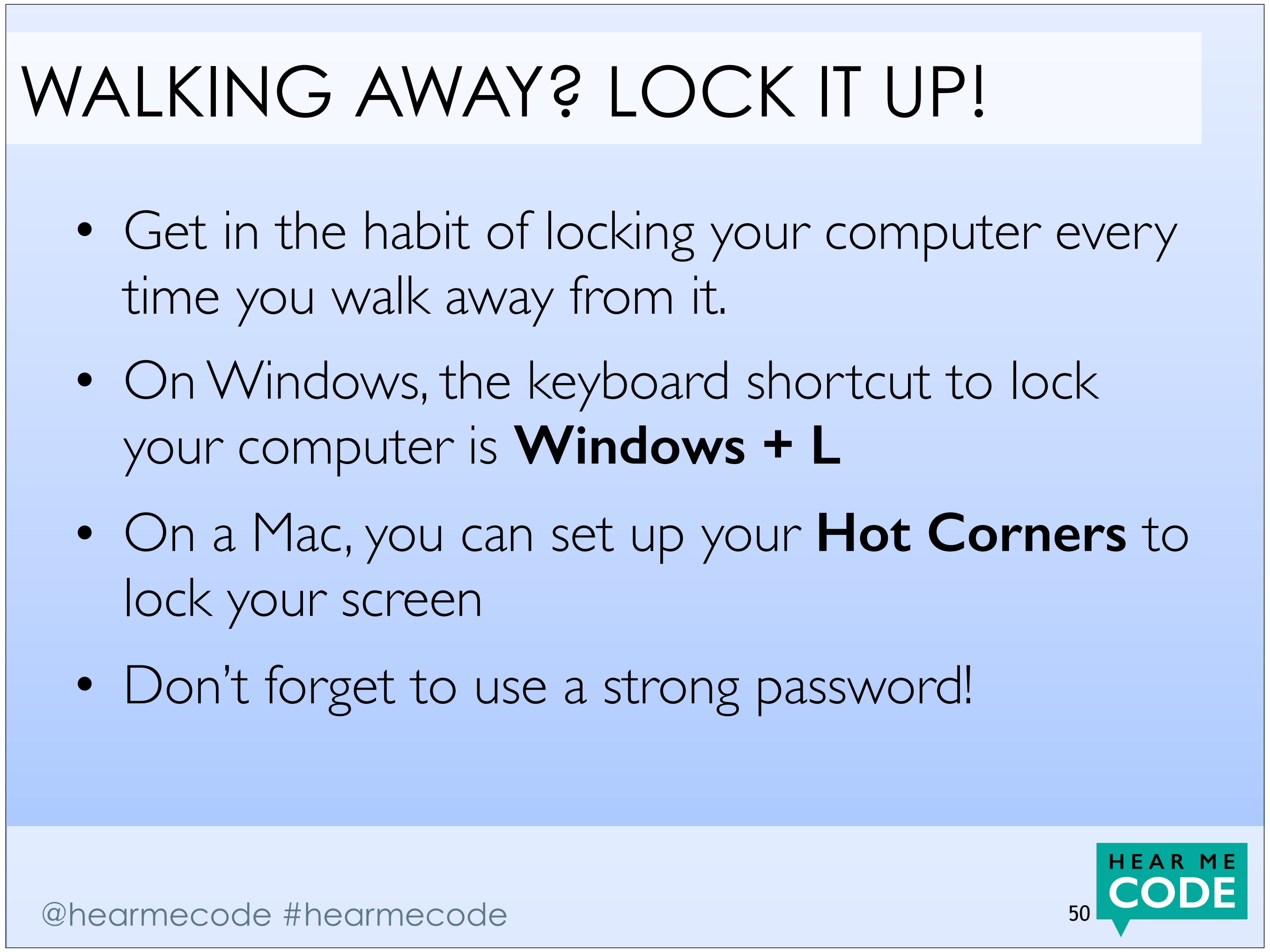
PASSWORD PROTECTING YOUR COMPUTER



SET A LOCK SCREEN WITH PASSWORD

- Make sure you need to enter a password to access your computer:
  - On startup
  - On waking up from sleep
  - On exiting the screensaver
- Set up a password-protected screensaver to start after a few minutes of inactivity

How many minutes of inactivity for your screensaver will depend on how you use your computer and what you’re trying to protect from, but keep in mind if anyone can physically access your computer without a password, they can in theory read all your emails, reset accounts, and so on.



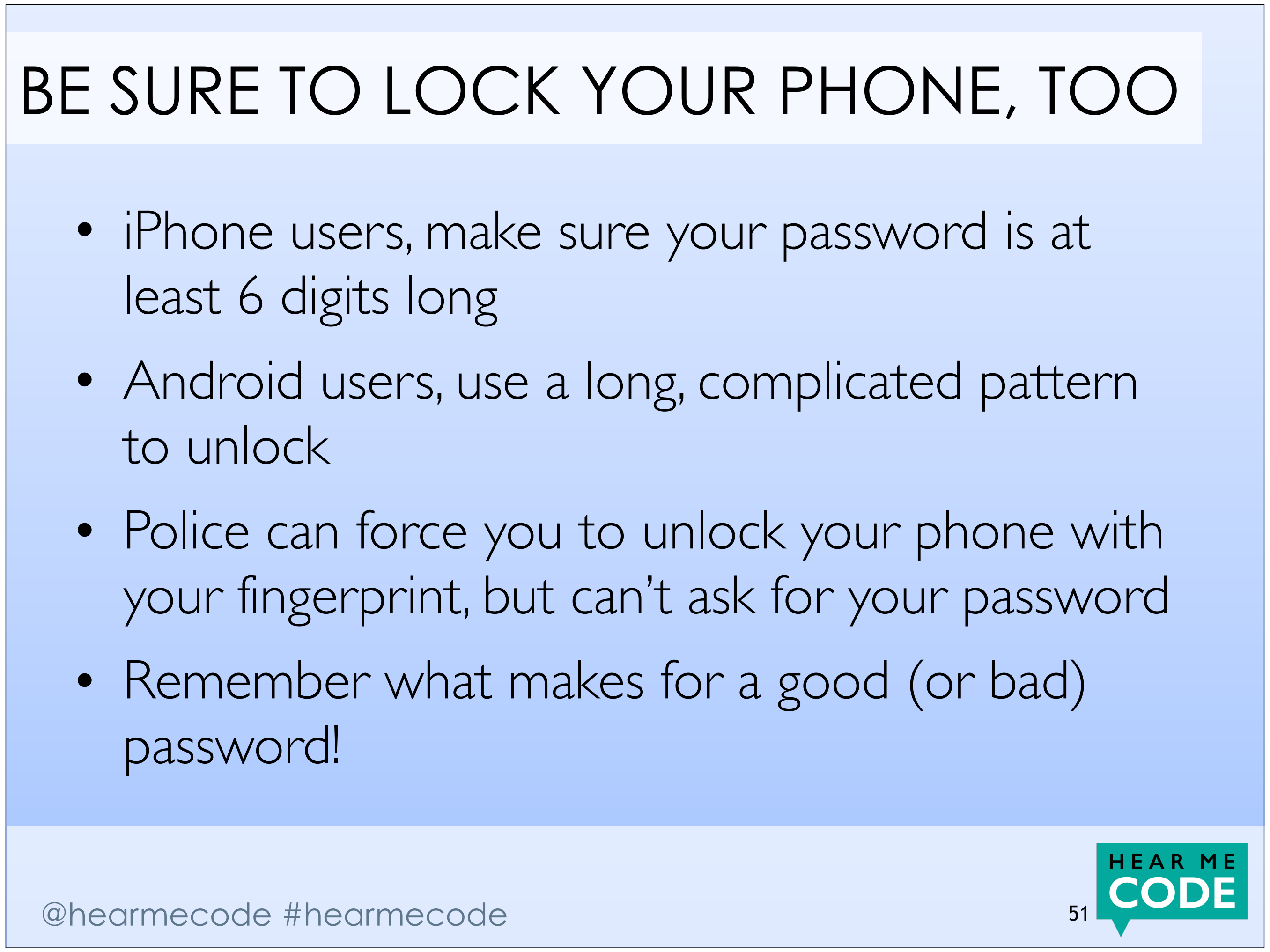
WALKING AWAY? LOCK IT UP!

- Get in the habit of locking your computer every time you walk away from it.
- On Windows, the keyboard shortcut to lock your computer is **Windows + L**
- On a Mac, you can set up your **Hot Corners** to lock your screen
- Don't forget to use a strong password!

@hearmecode #hearmecode

I have my Hot Corners set so when I move my mouse to the lower-right hand side of my screen, it will automatically lock my computer, which is very convenient.

To set your Hot Corners and Screen Saver, go to the Apple Menu > System Preferences, and in the top row, go to Desktop & Screen Saver > Screen Saver.



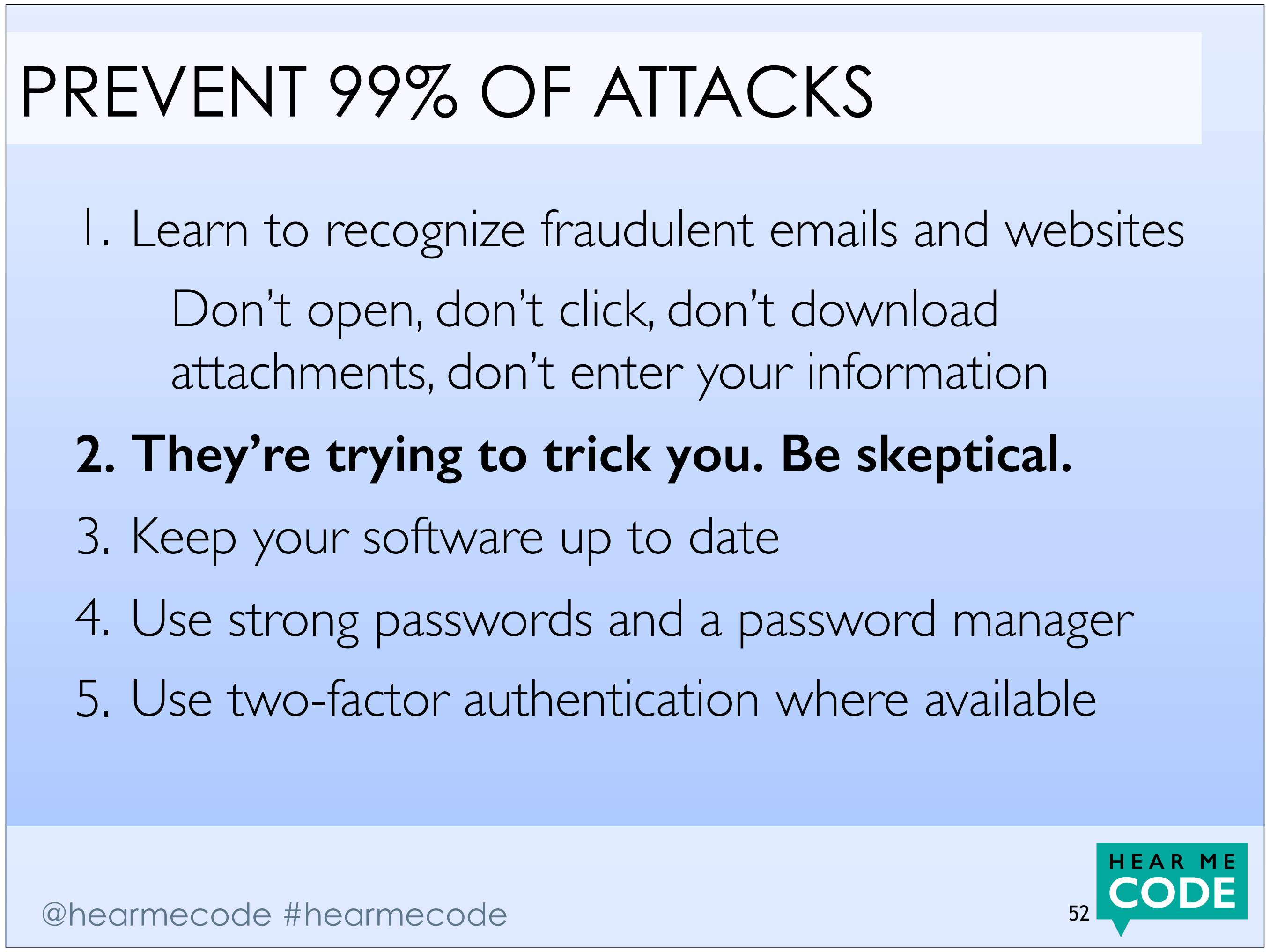
BE SURE TO LOCK YOUR PHONE, TOO

- iPhone users, make sure your password is at least 6 digits long
- Android users, use a long, complicated pattern to unlock
- Police can force you to unlock your phone with your fingerprint, but can’t ask for your password
- Remember what makes for a good (or bad) password!

@hearmecode #hearmecode

You’ll also want to configure your phone to lock itself after a certain period of inactivity. How long will depend on how you use your phone.

You might want to consider activating the feature that will erase all data on the phone after several failed password attempts to prevent someone from trying every password in the book.



PREVENT 99% OF ATTACKS

1. Learn to recognize fraudulent emails and websites

   Don't open, don't click, don't download attachments, don't enter your information

2. **They're trying to trick you. Be skeptical.**
3. Keep your software up to date
4. Use strong passwords and a password manager
5. Use two-factor authentication where available

This is maybe the most important slide, and is a good summary of everything we've covered.

CONTINUE LEARNING

Resources and additional trainings will be added here periodically.