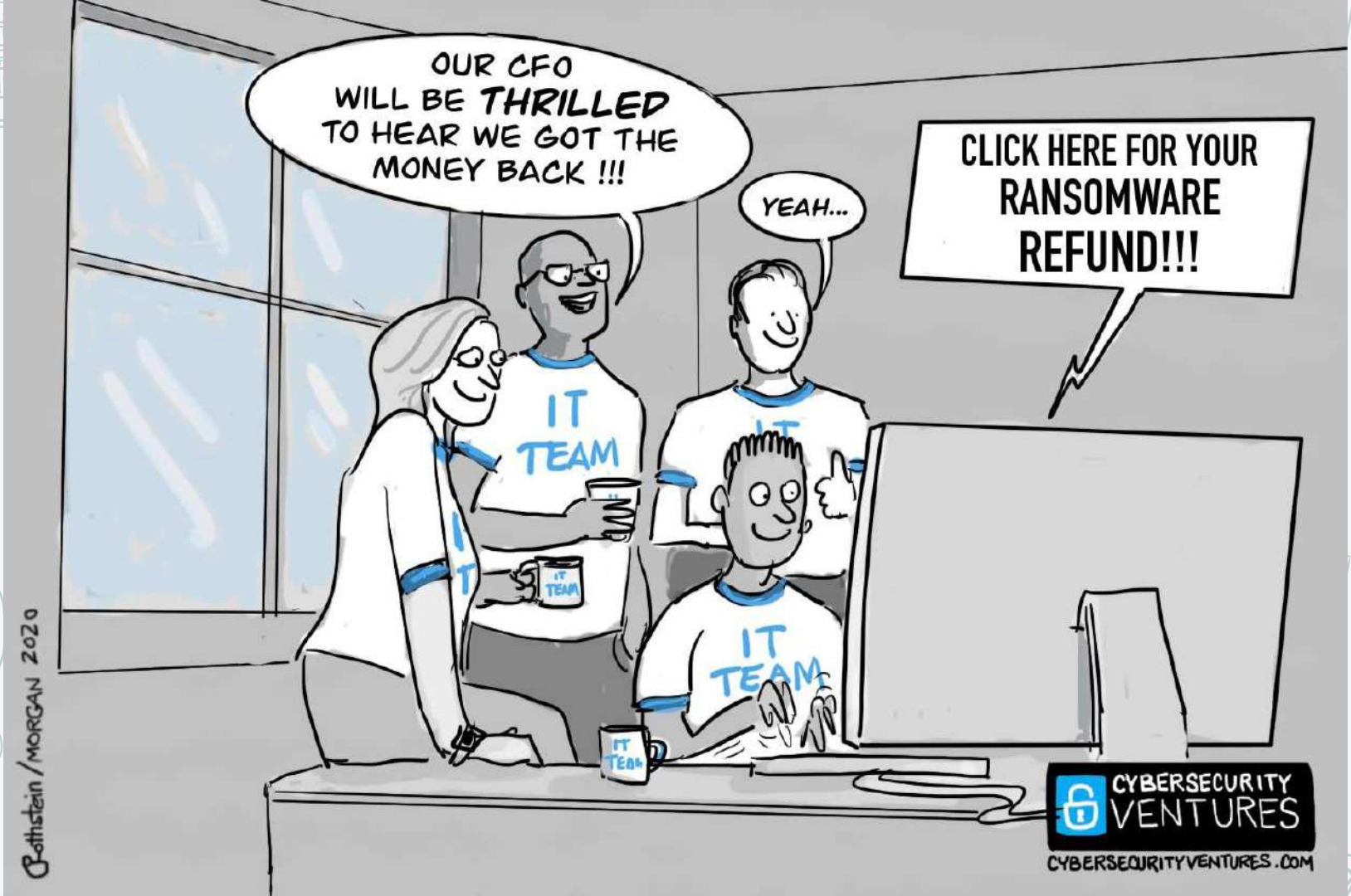
Cyber Security

Outline

TOPIC
1. Confidential Information
2. Choose a Password
3. Two-Factor Authentication
4. Malware, Viruses, and Spyware
5. Safely Install Software

TOPIC
6. Email and Phishing
7. Browse Securely
8. Social Media
9. Protect Your Computer's Data


OUR CFO WILL BE THRILLED TO HEAR WE GOT THE MONEY BACK !!!
YEAH...
CLICK HERE FOR YOUR RANSOMWARE REFUND!!!
IT TEAM
IT TEAM
IT TEAM
IT TEAM
IT TEAM
Bathstein / MORGAN 2020
CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM

Cyber Security

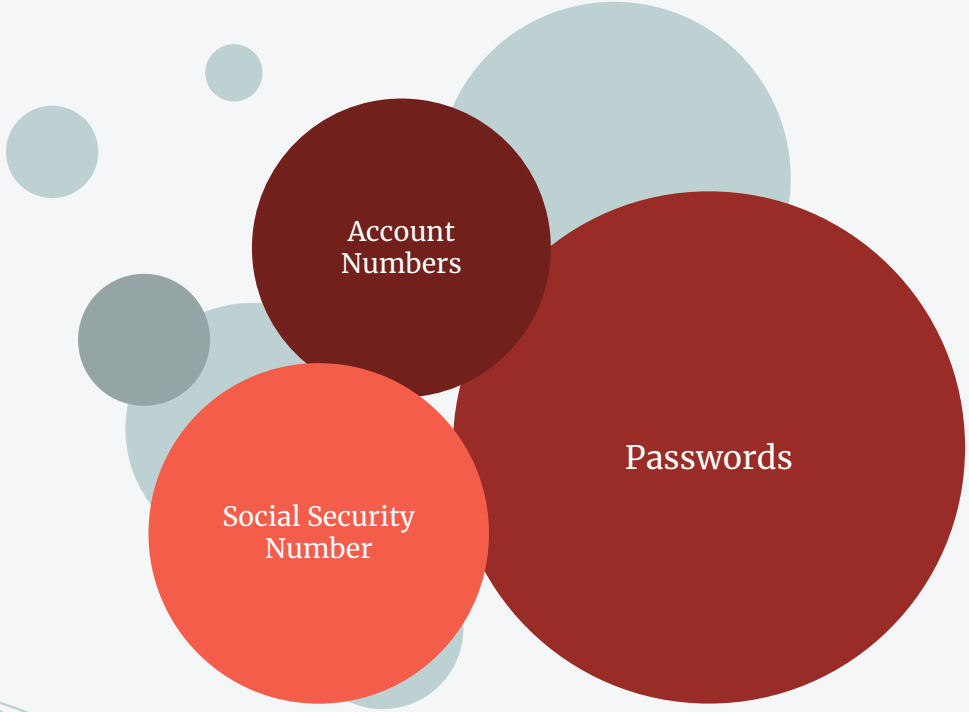
- 95% of cyber security breaches are due to human error.
- Human intelligence and behavior is the best defense against cyber attacks.

1.

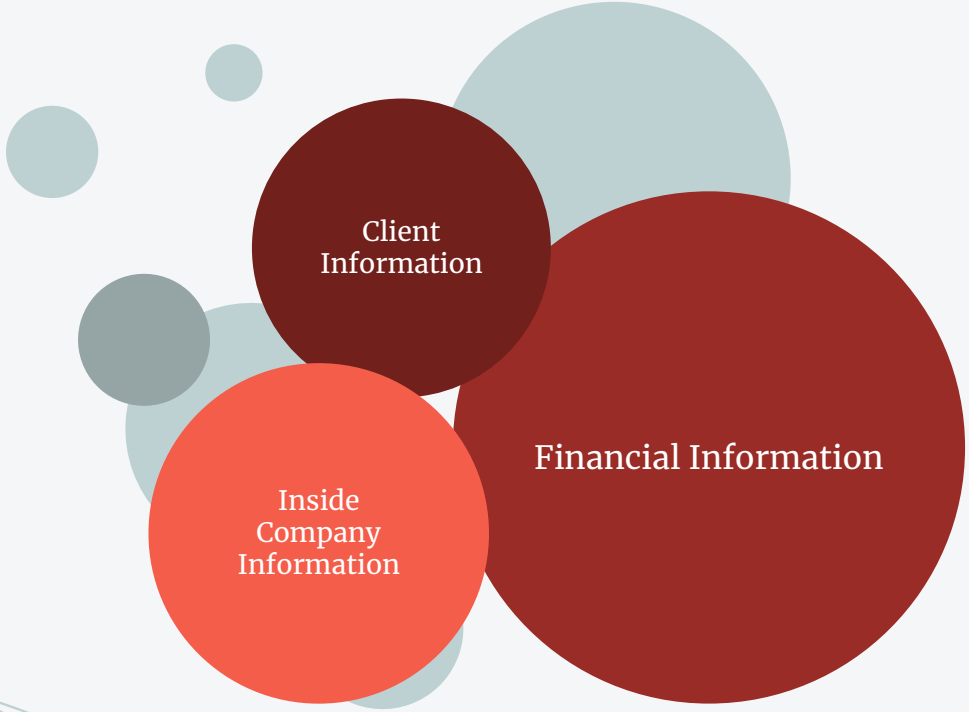
Confidential Information

Some information is more sensitive than others.

Confidential Personal Information

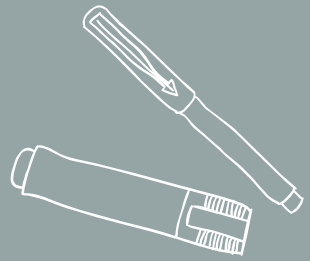
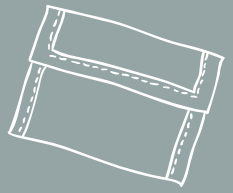


Confidential Work Information



Keep Confidential information Secure

- Never send confidential information through email.
- Use extreme caution when providing confidential information to a website.
- Keep your confidential information in a secure location.

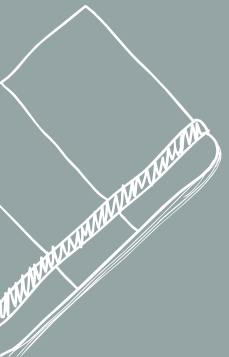



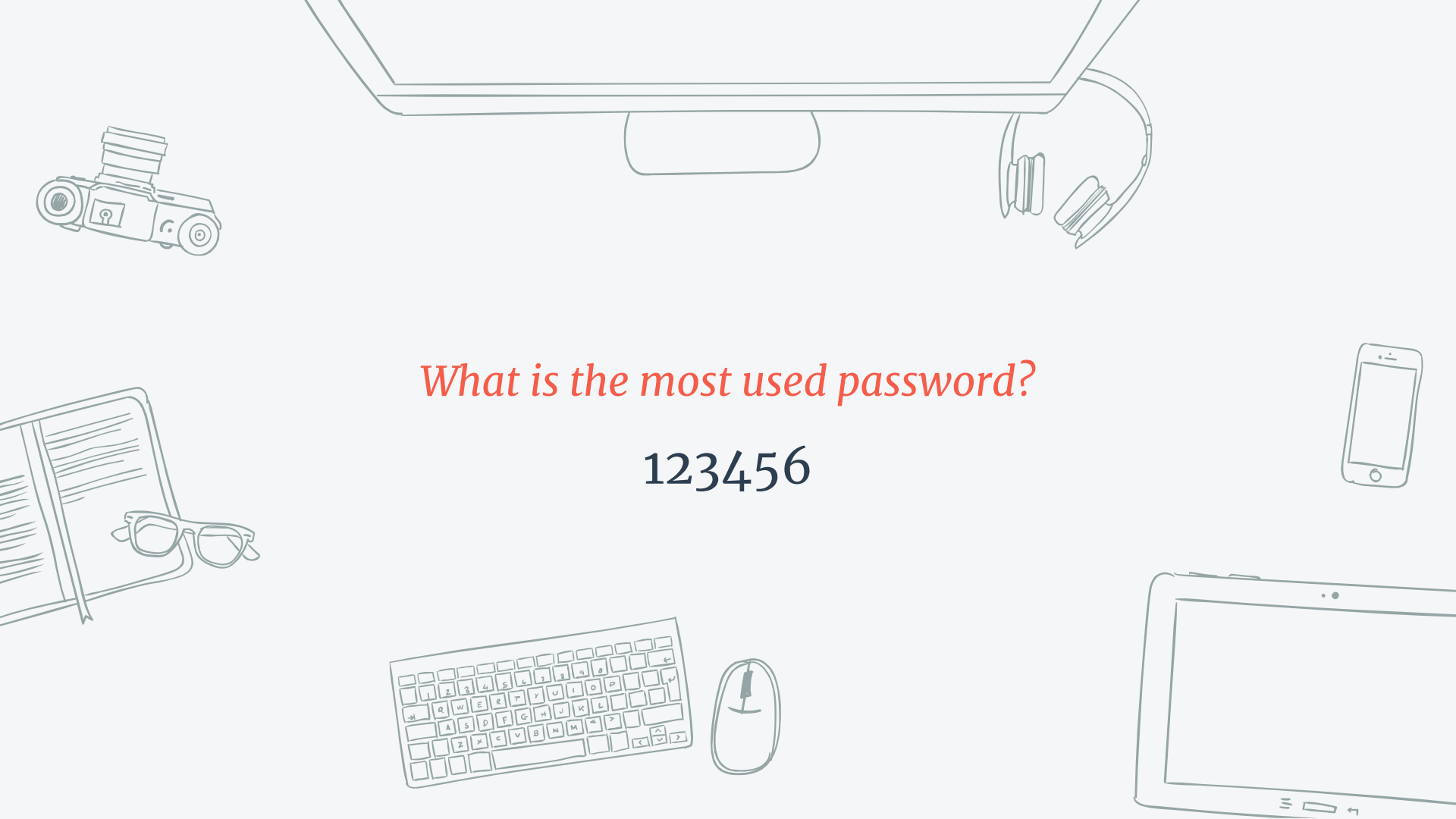

2.

Choose a Password

A password that is easy to remember is easy to hack.







What is the most used password?

123456

Choose a secure password

- Use at least 8 digits.
- Use a combination of both upper and lower-case letters.
- Include both a number and special symbol.
- Don't use the same password for all your accounts.
- Change your passwords every 3 to 6 months.

Password examples

Bad	Better	Best
accident	AcciDent	Acc!Den7
smellycat	sm3llycat	$m3llyc@t
creditunion	CreditUnion	Cr#ditUn1on

3.

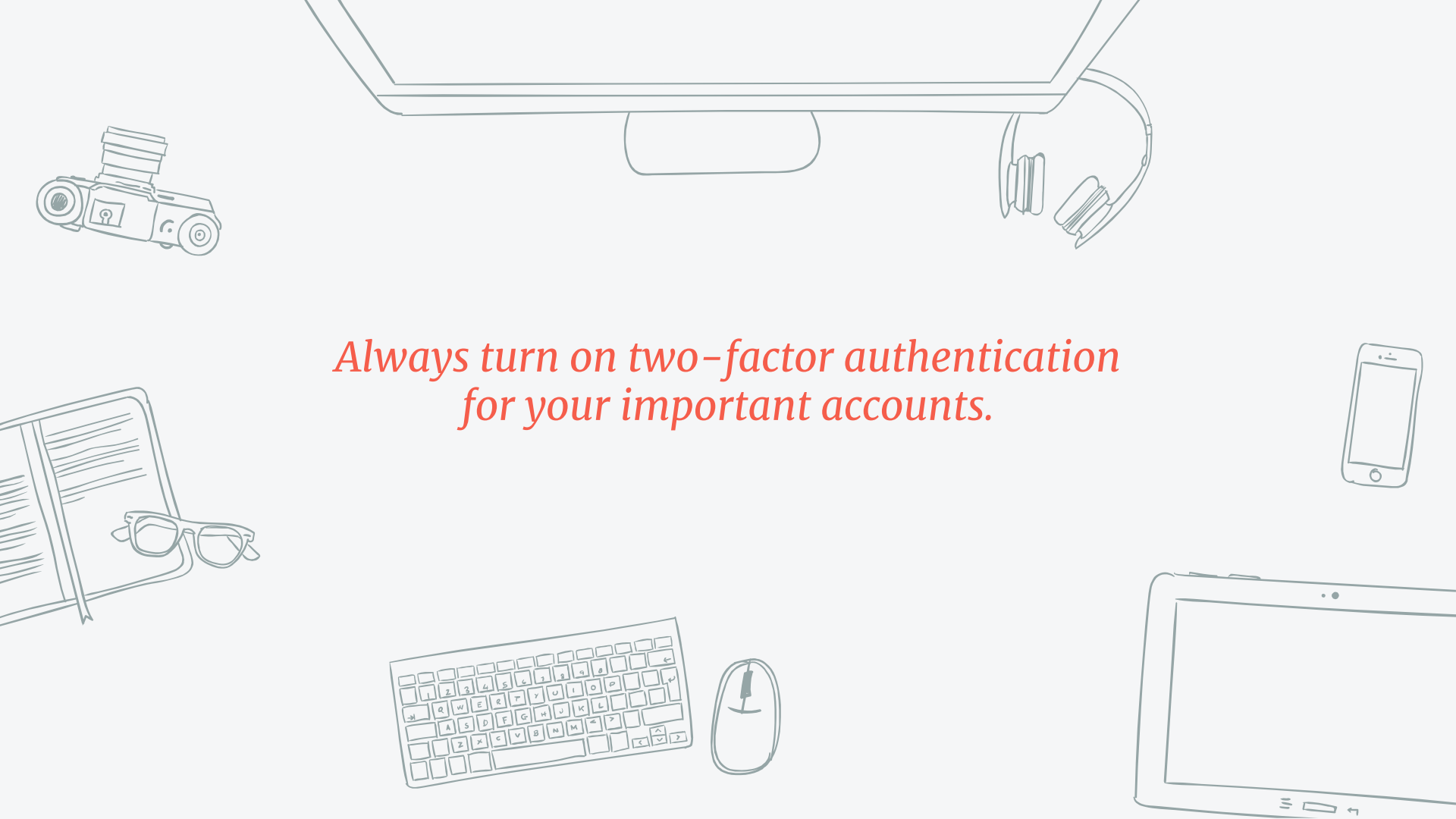
Two-Factor Authentication

Why aren't passwords good enough?

3 Recognized Factors for Authentication

1. Something you **know** (password).
2. Something you **have** (mobile phone).
3. Something you **are** (fingerprint).

Two-factor authentication
uses two of these options.

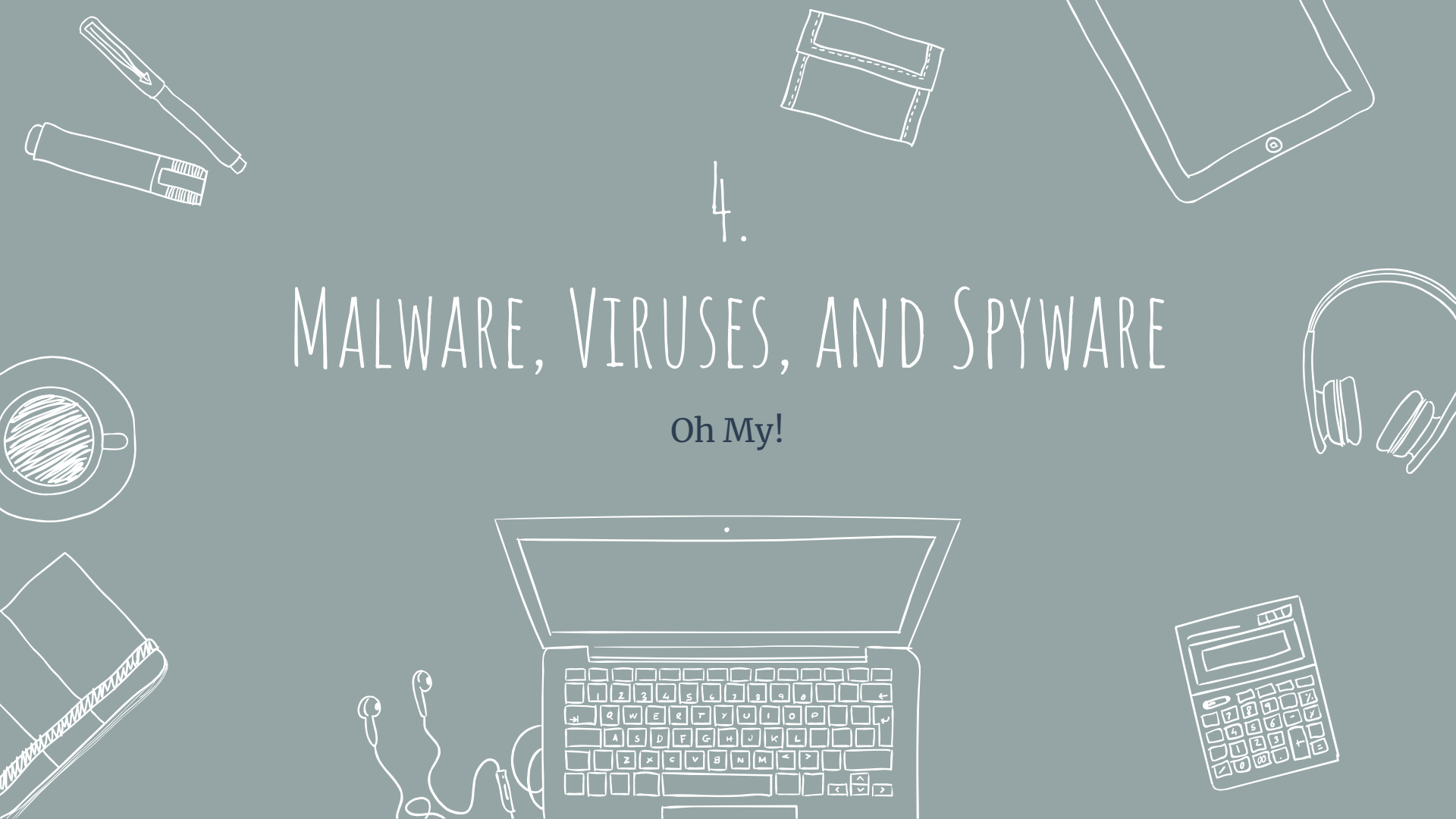


Always turn on two-factor authentication for your important accounts.

4.

Malware, Viruses, and Spyware

Oh My!



Malware

Malicious Software

Computer Virus

Computer programs that reproduce and infect other computers.

Adware

Hijacks your browser and forces it to display annoying advertisements.

Spyware

Secretly monitors all of your internet activity and sends your information to a third party.

Prevent malware

- Install antivirus / malware software.
- Keep your antivirus software up to date.
- Run regularly scheduled antivirus scans.
- Keep your operating system and software up to date.

5.

Safely Install Software

Make sure you're only installing the software you think you're installing.

Install Software the Safe Way

- Don't install personal software on company computers.
- Have up-to-date antivirus software.
- Make sure the software comes from a reliable source.
- Be careful when you install new software; decline any additional software you don't want.

6.

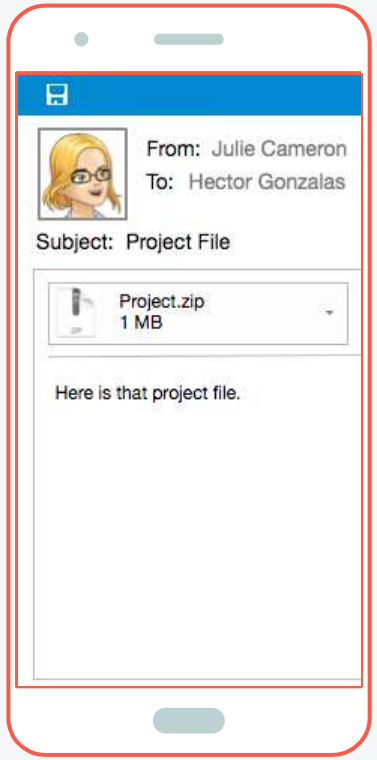
Email and Phishing

Very common and very difficult to identify.

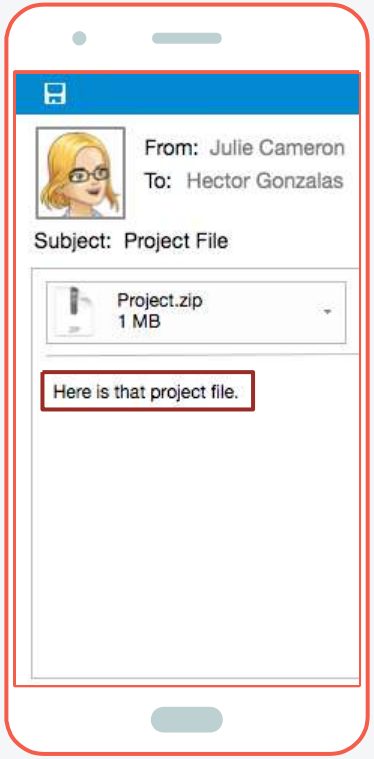
Phishing

Fake emails or websites used to trick people into revealing confidential information.


80%
of Americans could not distinguish
fake and legitimate emails

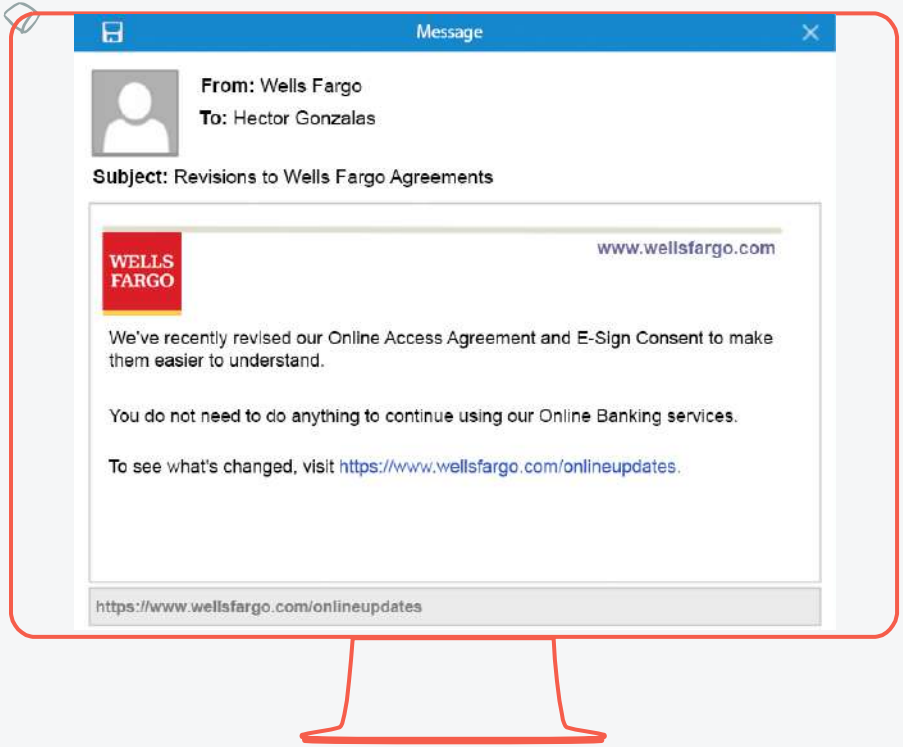

From: Julie Cameron
To: Hector Gonzalas
Subject: Project File
Project.zip
1 MB
Here is that project file.

Real or Fake?

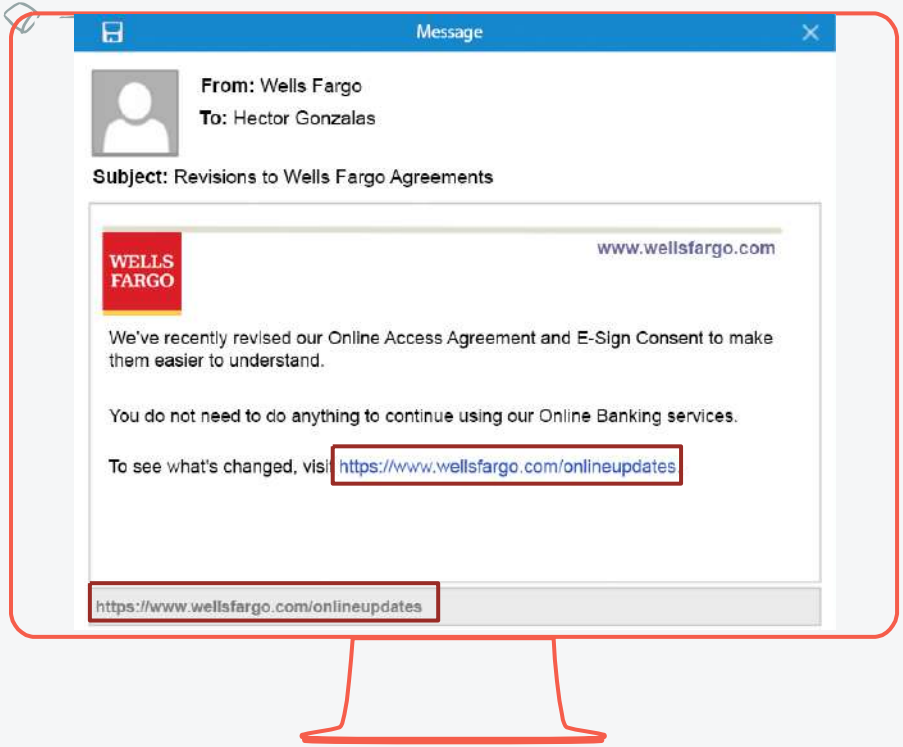


FAKE

Emails can appear to come from someone you know; but notice the vague message.

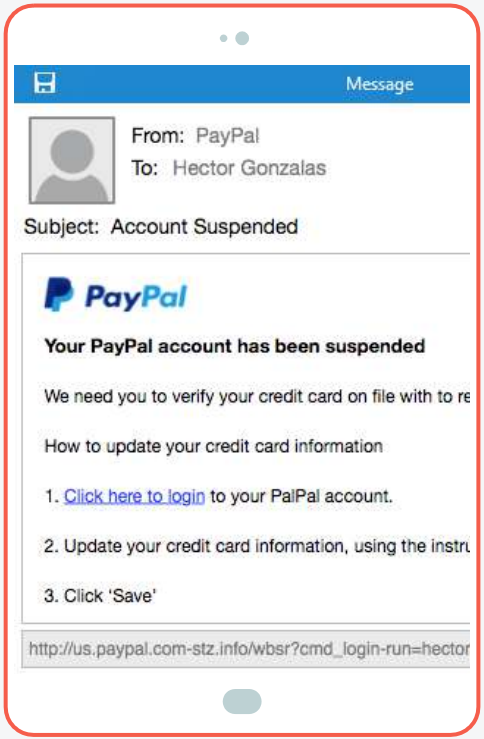

Message
From: Wells Fargo
To: Hector Gonzalas
Subject: Revisions to Wells Fargo Agreements
WELLS FARGO
www.wellsfargo.com
We've recently revised our Online Access Agreement and E-Sign Consent to make them easier to understand.
You do not need to do anything to continue using our Online Banking services.
To see what's changed, visit https://www.wellsfargo.com/onlineupdates.
https://www.wellsfargo.com/onlineupdates

Real or Fake?

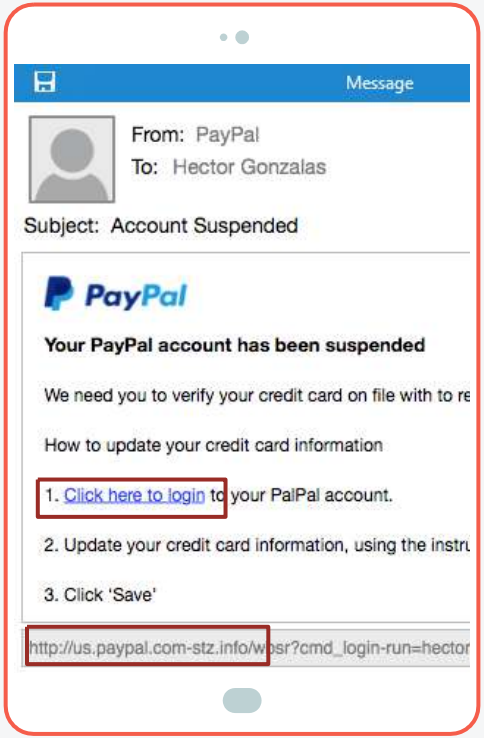


Real

Email is just informational, it's not asking you to do anything.
URL matches what's shown in the link.


Message
From: PayPal
To: Hector Gonzalas
Subject: Account Suspended
PayPal
Your PayPal account has been suspended
We need you to verify your credit card on file with to re
How to update your credit card information
1. Click here to login to your PalPal account.
2. Update your credit card information, using the instru
3. Click 'Save'
http://us.paypal.com-stz.info/wbsr?cmd_login-run=hector

Real or Fake?



FAKE

Link destination is not the official PayPal site.
Emails will usually not solicit you to change your password or login.

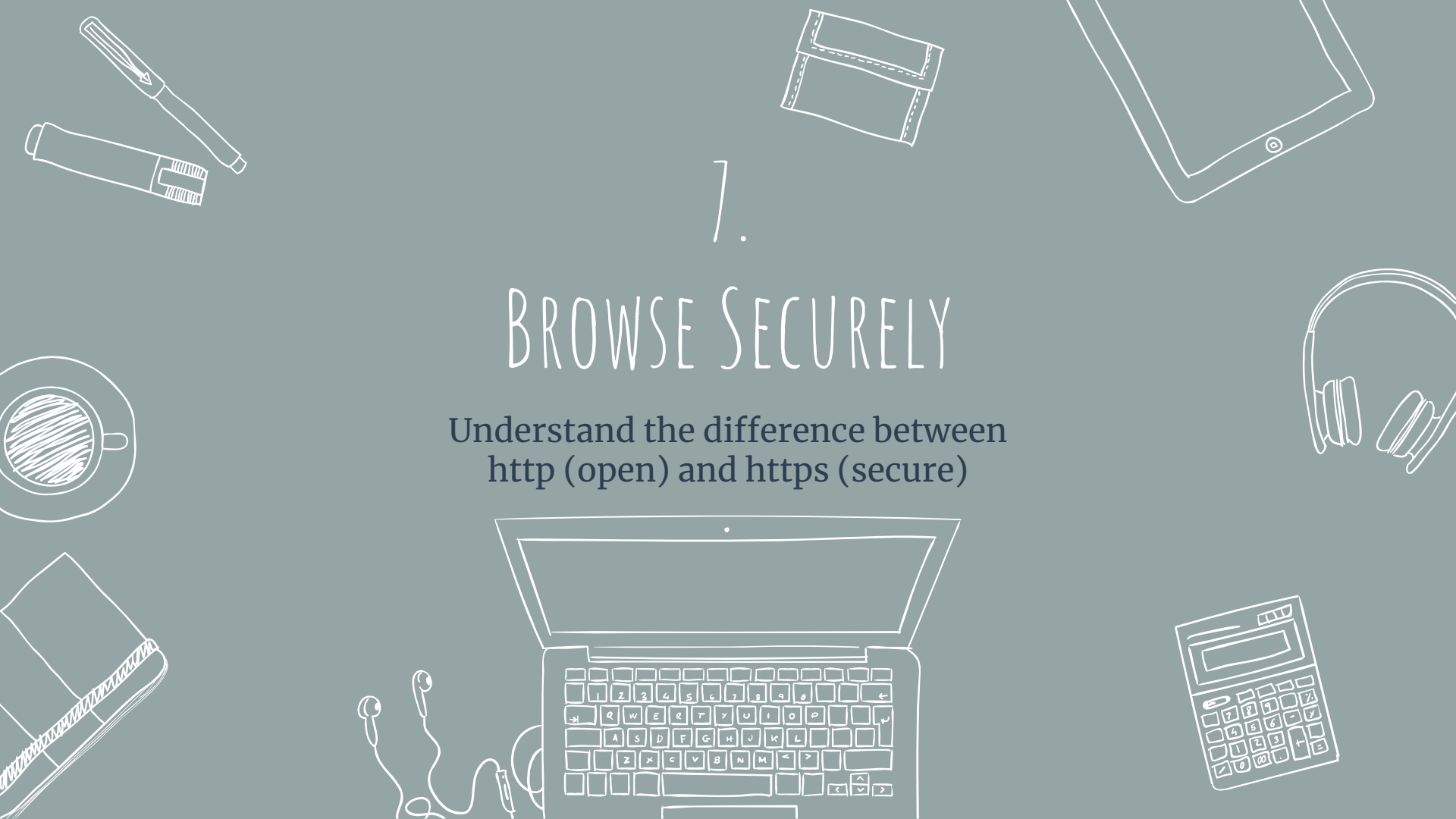
Email Security Tips

- Beware of phishing scams / fake emails.
- Unsolicited, legitimate emails will almost never ask you to login.
- Never open attachments in unsolicited or suspicious emails.

7.

Browse Securely

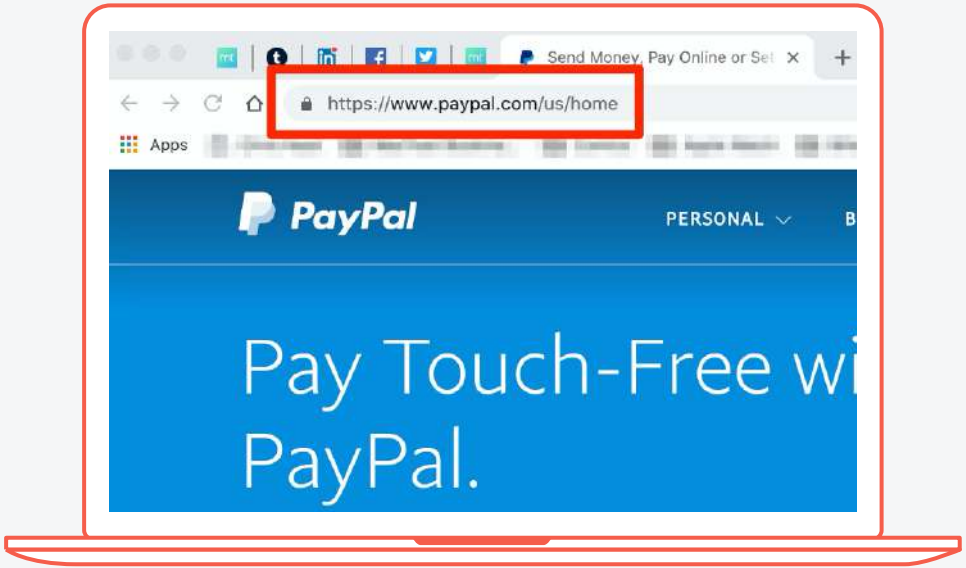
Understand the difference between
http (open) and https (secure)



https:

HTTPS

Secure, encrypted website.



HTTPS Sites

HTTPS and a lock icon appear in front of the site address in your browser.

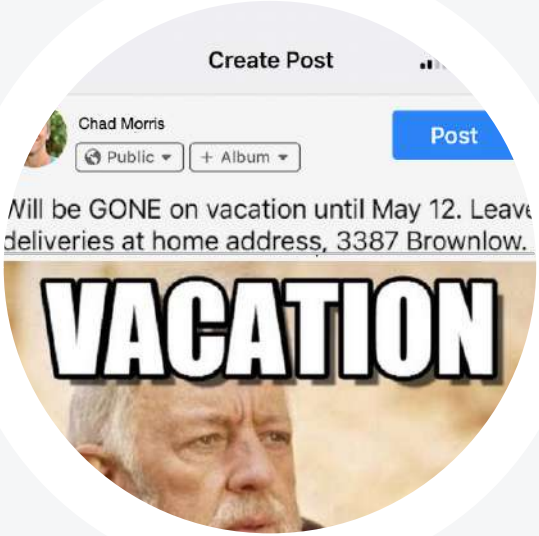
Make Sure You Are Using HTTPS When:

- Signing in; sending your user name & password.
- Making purchases; sending your credit card.
- Sending or working with confidential information.

8.

Social Media

Quick tips for staying safe.



Be careful what you post to social media

Keep personal information personal.

Social Media Safety Tips

- Adjust your privacy settings.
- Know and manage your friends.
- Keep personal information personal.
- Be mindful of your online reputation.

9.

Protect Your Computer's Data

How to keep your information safe, before a disaster.

Imagine Your Computer is Stolen

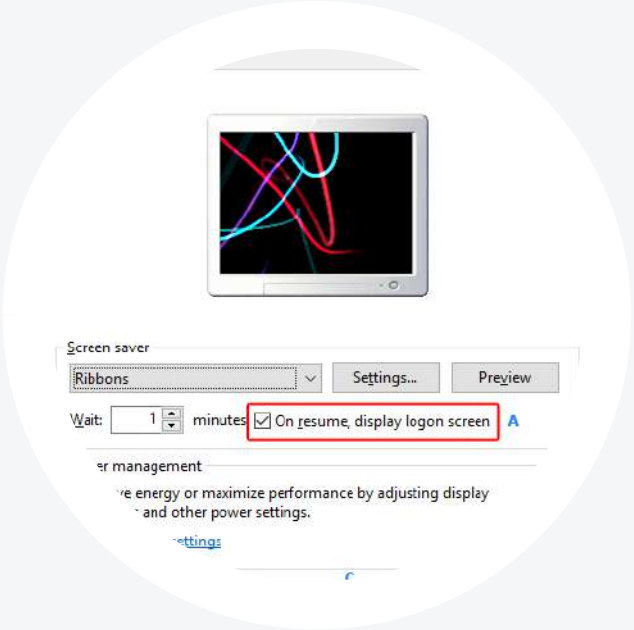
What could someone take from you if that happened?

A Lost or Stolen Computer Gives Someone Access To:

- The computer.
- Credentials to log into all your sites.
- Information about your financial accounts.
- Email and message history.
- Files and projects you've worked on.

Always require a login password

Prevent unauthorized access to your computer.



Require a password to resume from sleep

Keep your computer's information safe when you're away from it.

Backup your important files

Don’t lose hours of work if you lose your device.

Review

Let’s see what you’ve learned.

Question 1

Which of these does NOT need to be treated as confidential information?

A. Customer List
B. Company Website
C. Business Process
D. Employee Information

Question 1

Which of these does NOT need to be treated as confidential information?

A. Customer List
B. Company Website
C. Business Process
D. Employee Information

A company's website is not confidential information.

Question 2

True or False: It's recommended to use the same password for all of your accounts so it's easy to remember.

Question 2

True or False: It's recommended to use the same password for all of your accounts so it's easy to remember.

False: You should always use a different password for each account.

Question 3

Which of the following is a common type of malware?

A. Virus
B. Adware
C. Spyware
D. All of the above

Question 3

Which of the following is a common type of malware?

A. Virus
B. Adware
C. Spyware
D. All of the above

All of these are common types of malware.

Question 4

True or False: A phishing scam downloads malicious software on your computer.

Question 4

True or False: A phishing scam downloads malicious software on your computer.

False: A phishing scam is designed to trick you into providing your confidential data to steal money or information.

Question 5

Which of the following is NOT something you should do when backing up your data?

A. Make sure your files are saved off-site
B. Routinely verify backups
C. Copy and paste all your files to the desktop
D. Use automated backup software

Question 5

Which of the following is NOT something you should do when backing up your data?

A. Make sure your files are saved off-site
B. Routinely verify backups
C. Copy and paste all your files to the desktop
D. Use automated backup software

Copying and pasting your files to the desktop is not a means of backup.