10 WAYS TO PROTECT YOURSELF ONLINE

Computer Security

- You can have great Security
- You can have great Convenience
- ***But, you can't have both***

Computer Security

- The Goal: Balance
  - Good Security *and* Nice Convenience

Computer Security

- There are many ways to Protect Yourself
- These are just the Top Ten

10

Which Is More Secure?

A. Your PC

B. Your Cellphone

Which Is More Secure?

A. Your PC

- Bigger
- More powerful
- Easy to install apps

B. Your Cellphone

- Harder to install apps

Which Is More Secure?

A. Your PC

- Bigger
- More powerful
- Easy to install apps

B. Your Cellphone

- Harder to install apps
- **Thus, harder to install viruses**

If you need to open any strange email ...

Open it on your cellphone

10. USE MOBILE DEVICES

9

Do You Know What This Is?

Hak5
WiFi Pineapple

$119.99

“WiFi Auditor”

Can spy on nearby WiFi users

At your
local coffee
shop

Someone could
be eavesdropping
on your
communication

What Can We Do?

- Use a VPN app on your laptop
- VPN = Virtual Private Network
- Your connection will now be encrypted

Which VPN?

- IVPN
- TunnelBear
- ExpressVPN

9. USE A VPN

8

“Digital marketing experts estimate that most Americans are exposed to around 4,000 to 10,000 ads each day.”

– Forbes.com, Aug. 2017

Worst Problem of Online Ads?

A. Annoying

B. Slows down website appearance

C. Can infect your PC

Worst Problem of Online Ads?

A. Annoying

B. Slows down website appearance

C. Can infect your PC

How Can This Happen?

- Ads are sold and distributed by computers
- Many are never examined by humans
- Hackers can take advantage of this:
  - “Name-brand” ad takes you to a malicious site
  - Any click will download a virus onto your PC

What Can We Do?

- Avoid sites with excessive ads

  Or

- Use an Ad-Blocker app
  - But use it carefully
  - Websites depend on advertising
  - Ad-Blockers cut off their revenue

Which Ad-Blocker?

- Ublock Origin

8. USE AN AD BLOCKER

7

Computer Programs Are Huge

- Millions of lines of computer code
- Some lines can be mistakes
- Mistakes can give access to hackers

Fixing the Problem

- Companies constantly checks for mistakes
- They fix each mistake when found
- They offer updates to users

Meanwhile, in *Romalvania* ...

- Hackers watch for these updates
- Design programs to exploit the mistake
- Prey upon people who ***don't update***

What Can We Do?

- Be sure your programs are up to date
- Use auto-update features if available

7. KEEP YOUR PROGRAMS UP TO DATE

6

What's Better Than a Password?

- A Password

  and

- Something Else
- Called "Two-Factor Authentication"
- Or: Multi-Factor Authentication (MFA)

Two-Factor Authentication

1. Something you *know*
   - The Password
2. Something you *have*
   - The Second Factor

Second Factors Can Be:

- Message sent to your cellphone
- An Authenticator app on your phone
- An Authenticator dongle
- A list of one-time emergency passwords

6. USE TWO-FACTOR AUTHENTICATION

5

What Do You Post on Facebook?

- Birthdates
- Relatives’ names
- Children’s names
- Pets’ names
- Vacations

What Do You Post on Facebook?

- Birthdates
- Relatives' names
- Children's names
- Pets' names
- Vacations

What's the Problem?

- Hackers can access social media
- Can develop profiles of you
- Can steal your identity
- Can possibly guess passwords
- Rob your home when you are away

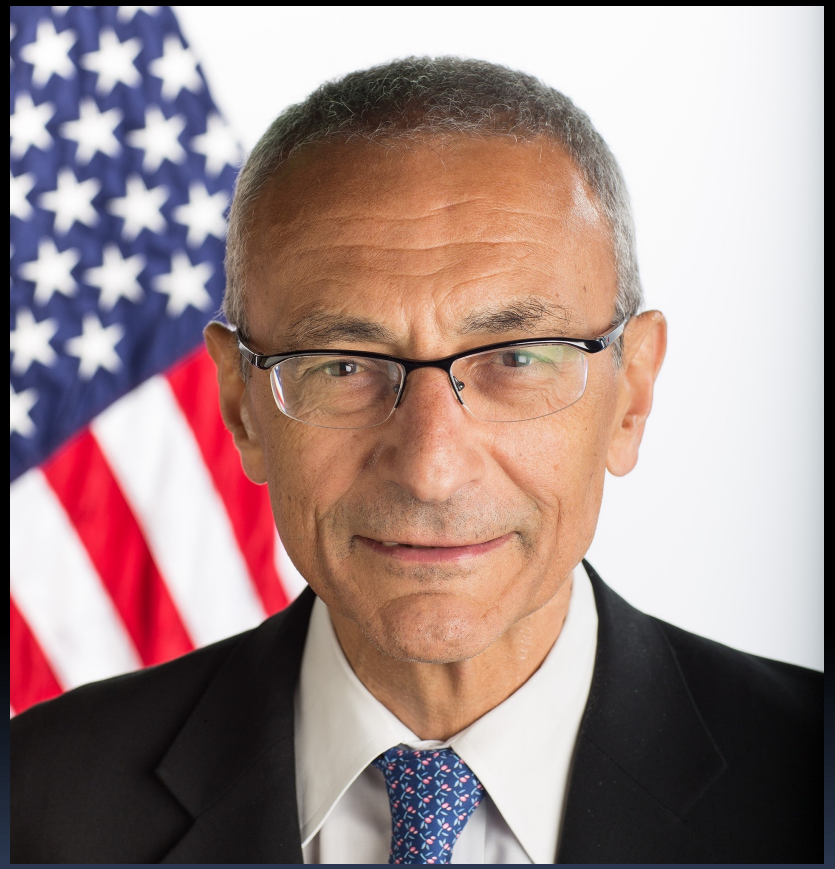
What Can We Do?

- Have fun on Social Media
- But, limit the personal info you share

5. BE WARY OF SOCIAL MEDIA

4

Do you know this man?



John Podesta
Chairman, Clinton for President

Hillary Clinton

Anything wrong with this email?

The following slide shows the actual email received by Mr. Podesta

From: Google <no-reply@accounts.googlemail.com
Date: March 19, 2016 at 4:34:30 AM EDT
To: jpodesta@gmail.com
Subject: *Someone has your password*

Someone has your password
Hi John
Someone just used your password to try to sign in to your account jpodesta@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 https://bit.ly/1PibSU0

Best,
The Gmail Team

From: Google <no-reply@accounts.googlemail.com
Date: March 19, 2016 at 4:34:30 AM EDT
To: jpodesta@gmail.com
Subject: *Someone has your password*

Someone has your password
Hi John
Someone just used your password to try to sign in to your account jpodesta@gmail.com.

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

Subject: "Someone has your password

Someone has your password
Hi John
Someone just used your password to try to sign in to your account jpodesta@gmail.com.

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

Ironic!

Good Idea!

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

CHANGE PASSWORD https://bit.ly/1PibSU0

Subject: "Someone has your password

Someone has your password
Hi John
Someone just used your password to try to sign in to your account jpodesta@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 https://bit.ly/1PibSU0

Very Strange!

bit.ly

- Is used to shorten web addresses
- But, can also ***hide*** suspicious addresses

Mr. Podesta did exactly what he should have done.

He forwarded the note to his IT support person.

The following slide shows the actual reply from the IT support person.

Subject: Re: Some has your password

Sara,

This is a legitimate email. John needs to change his password immediately and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.goog.e.com/security to do both. It is absolutely imperative that this is done ASAP.

If you or he has any questions, please reach out to me at 410-562-9762.

Unfortunately, the IT support person left out one word.

Subject: Re: Some has your password

Sara, NOT

This is a legitimate email. John needs to change his password immediately and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.goog.e.com/security to do both. It is absolutely imperative that this is done ASAP.

If you or he has any questions, please reach out to me at 410-562-9762.

Subject: Re: Some has your password

Sara, NOT

This is a legitimate email. John needs to change his password immediately and ensure that two-factor authentication is turned on his account.

Good link

He can go to this link: https://myaccount.goog.e.com/security to do both. It is absolutely imperative that this is done ASAP.

If you or he has any questions, please reach out to me at 410-562-9762.

But, believing the first message was *legitimate*, Mr. Podesta went back to it.

And clicked the *bit.ly* link.

This probably took him to a site that looked like a Google page.

He changed his password.

But, the hacker now knew his password.

A few days later, all of Mr. Podesta’s email appeared on a public website.

Many messages contained embarrassing details.

Some people believe that Hillary Clinton lost the 2016 presidential election ...

... because someone clicked the wrong link.

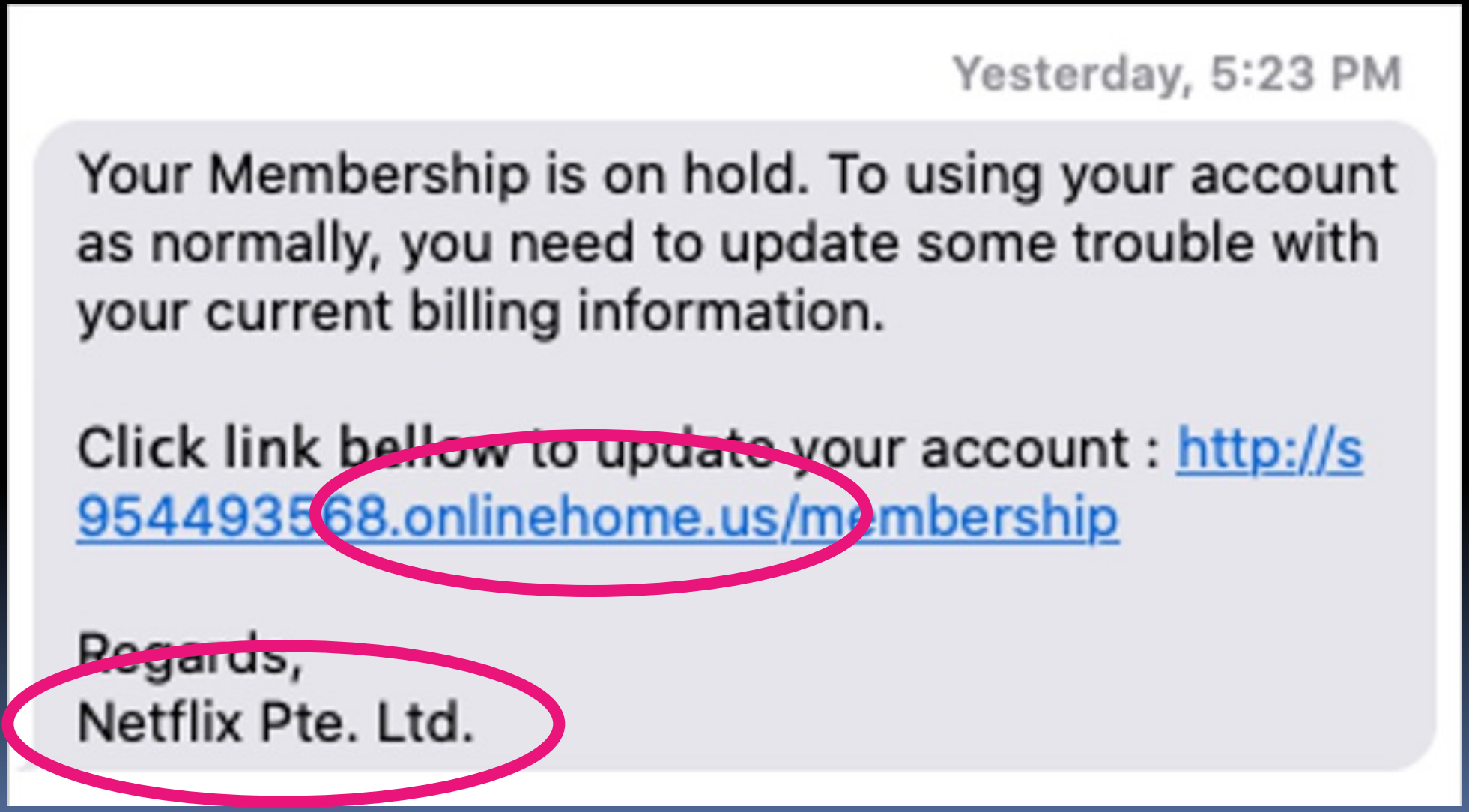
This Is Called "**Phishing**"

- Fake Email or Web sites
- Tricks Internet users to reveal:
  - Credit card, Social Security numbers, etc.

Here is another example.

This time, a text message I received recently.

Is This Text Message From Netflix?



We Checked This on Google

- Onlinehome.us
  - Many people reported that this domain is used for scams
- Netflix Pte. Ltd.
  - This the local branch of Netflix in ***Singapore***

YOUR COMPUTER HAS BEEN LOCKED!

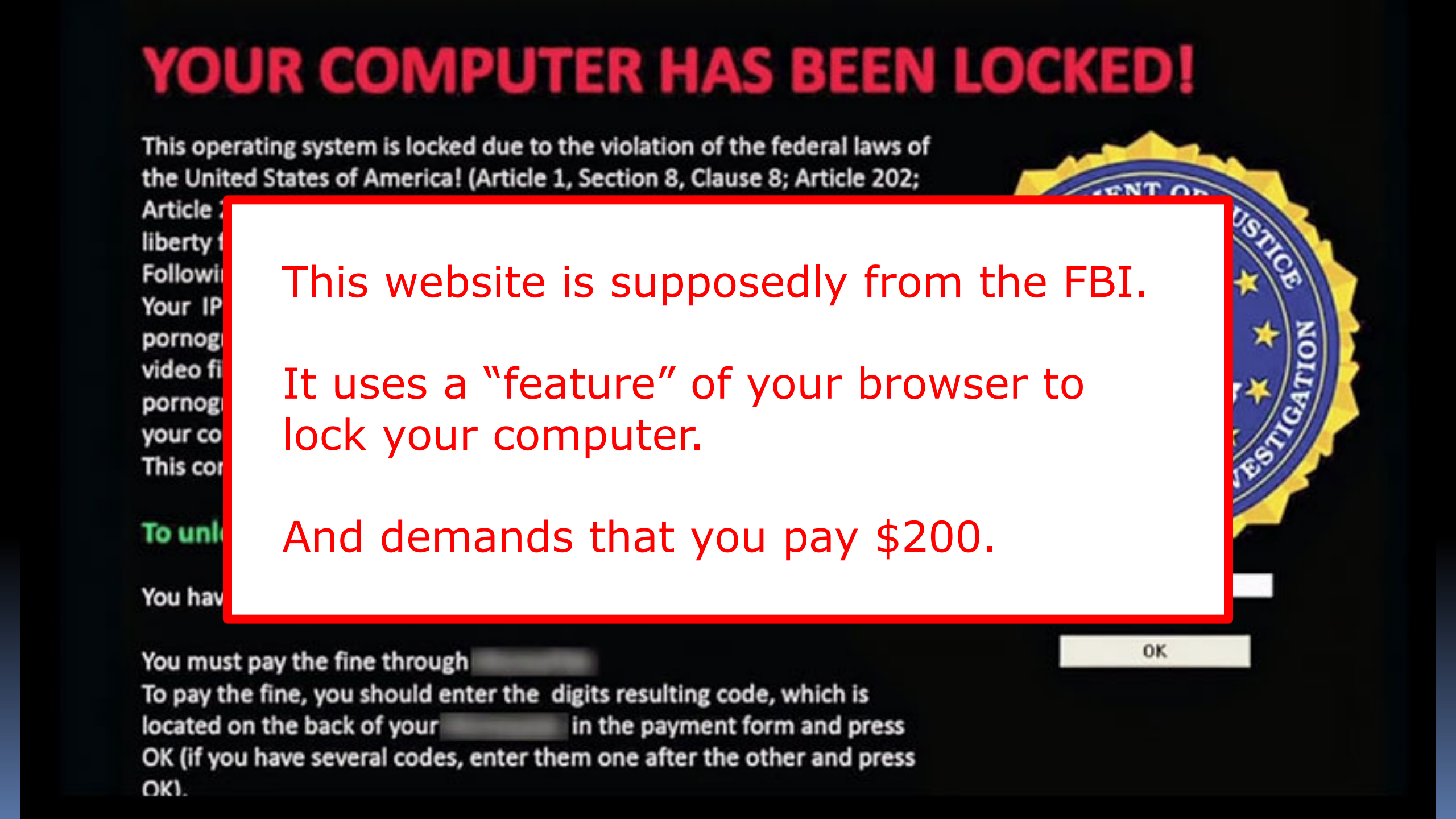
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

OK


YOUR COMPUTER HAS BEEN LOCKED!
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202;
Article
liberty
Followi
Your IP
pornog
video fi
pornog
your co
This cor
To unl
You hav
OK
You must pay the fine through
To pay the fine, you should enter the digits resulting code, which is located on the back of your in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
This website is supposedly from the FBI.
It uses a "feature" of your browser to lock your computer.
And demands that you pay $200.

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of
liber
Follo
Your
porn
vide
porn
your
This

To u

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

OK

If this happens to you,

Just turn off your computer and restart it.

Everything will be back to normal

4. BE SUSPICIOUS

3

The next slide is one of the scariest things you may see on your computer.


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Check Payment

Decrypt

What Happened?

- A ransomware has infected your PC
- Encrypted all your data
- You must pay to get your data back

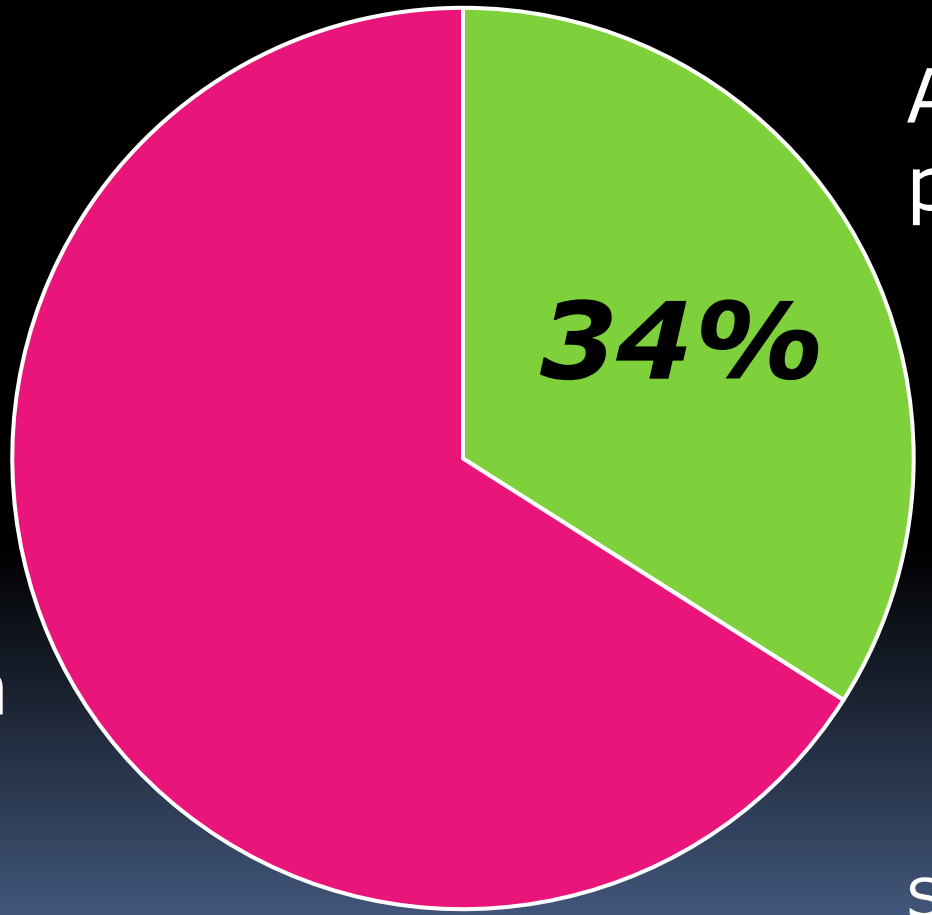
A Better Alternative

- Ignore the ransom threat

What About Your Data??

- Use your backup data

How Many People Back Up Their Data?



At least once per month

Less often or never

Source: statista.com, 2018

Backups Save Us From:

- Ransomware or Virus attacks
- Equipment failures
- Lost or stolen laptops
- Fire or flood damage
- Accidental data erasures

What Can We Do?

- Use an external hard drive
  - About $70 at Staples/Amazon
- Or, Use an Online Backup service
  - E.g., Carbonite, about $70/year
- Or, Use both

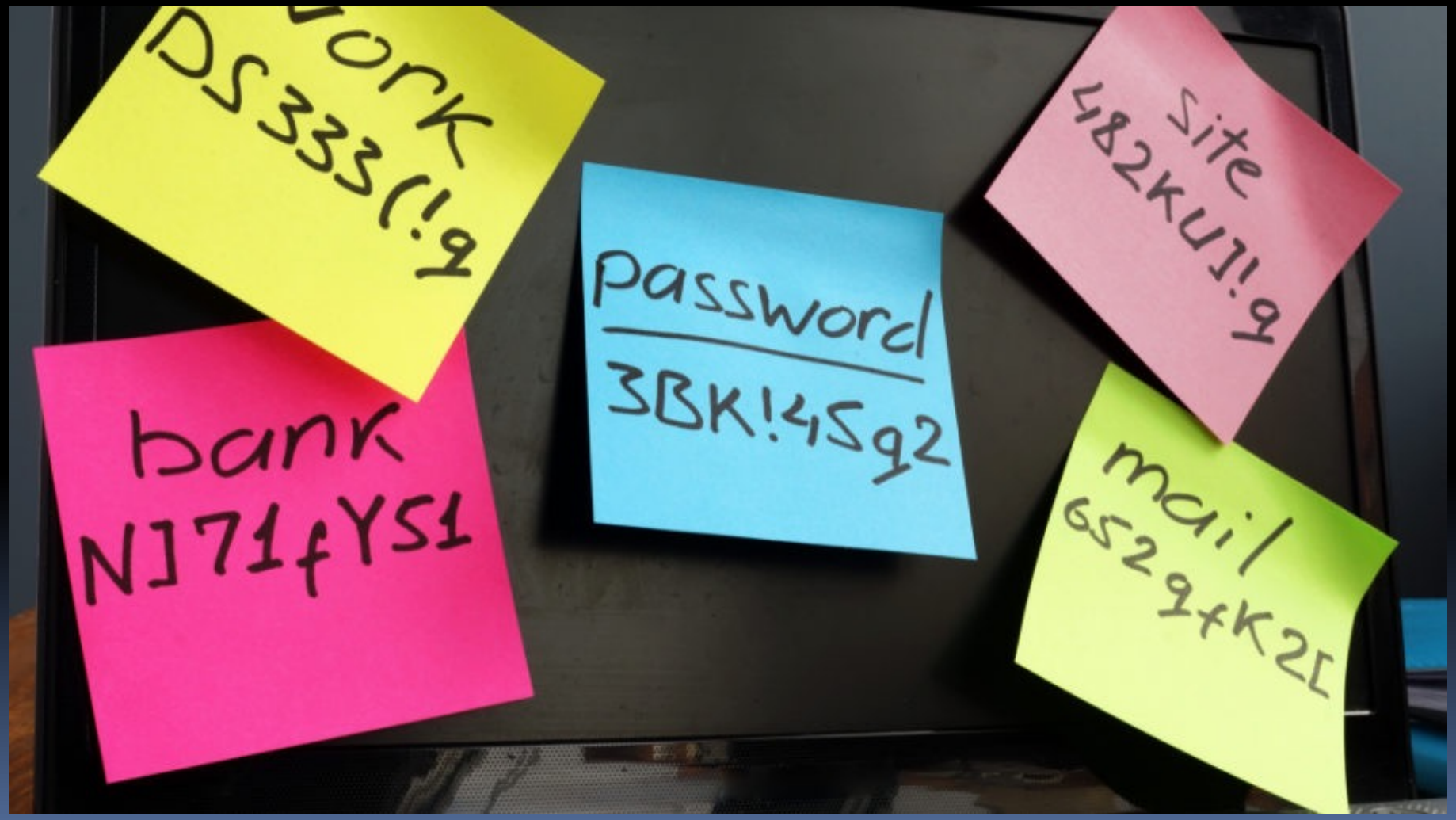
Low-Cost Backup

- 128GB USB Flash Drive (memory stick): $13
- iDrive online backup, 10GB: Free

3. BACK UP YOUR DATA

2

How Do You Keep Track of Your Passwords?



Where Do You Store All Your Passwords?

A. Sheets of paper

B. Notebook

C. My computer

D. In Email messages

What Can We Do?

- Use a Password Manager
- Examples:
  - 1Password
  - Dashlane
  - LastPass

What Do Password Managers Do?

- Store all your passwords online
- Enter passwords into forms automatically
- Only you can access them
  - Only you have the password
  - Even the FBI cannot get access

For Extra Security …

- For really important accounts ($$$):
  - Add a nonsense character at end of password
  - Remember to delete this character later
- Even if hackers break into your password vault
  - They still cannot access your key accounts

2. USE A PASSWORD MANAGER

Recap: 10 Ways to Protect Yourself Online

10. Use Mobile Devices
9. Use a VPN
8. Use an Ad-Blocker
7. Keep Your Programs Up to Date
6. Use Two-Factor Authentication
5. Be Wary of Social Media
4. Be Suspicious
3. Back Up Your Data
2. Use a Password Manager

1

What Is Your First and Often Only Defense Against Hackers?

PASSWORDS

In 2013, hackers broke into Adobe’s website.

They gained access to 153 million accounts.

The next slide shows the 10 most common passwords chosen by Adobe users.

Top Ten Passwords at Adobe

Most Popular Passwords
Among 130 million Adobe users
From: http://stricture-group.com/files/adobe-top100.txt
Nov. 2013

Rank	Password	Count
1	123456	1,911,938
2	123456789	446,162
3	password	345,834
4	adobe123	211,659
5	12345678	201,580
6	qwerty	130,832
7	1234567	124,253
8	111111	113,884
9	photoshop	83,411
10	123123	82,694

Many people use very weak passwords.

A Strong Password

- Think of a strong password, but easy to remember
- Write it down
- Let’s test how strong it is

Is Your Password Strong?

- Password strength tests:
  - www.grc.com/haystack.htm
  - www.PasswordMeter.com

What Is a Strong Password?

- At least 14 characters
- Include different characters:
  - Capitals, Numbers, Symbols
- Randomly chosen
  - Avoid common words, dates, names
- Change the password regularly

These rules have recently been revised.

What Is a Strong Password?

- At least 14 characters
- Include different characters:
  - Capitals, Numbers, Symbols
- Randomly chosen
  - Avoid common words, dates, names
- ~~Change the password regularly~~

  Change passwords only when needed

Can You Remember This Password?

4Sa7ya,ofbfotc

Can You Remember This Password?

4Sa7ya,ofbfotc

4 Score **a**nd **7 y**ears **a**go**, o**ur **f**orefathers
brought **f**orth **o**n **t**his **c**ontinent

Some Major Data Breaches

JP Morgan Chase	2014	76 Million
Equifax	2017	146 Million
Adult Friend Finder	2016	412 Million
Marriott	2018	500 Million
Facebook	2021	530 Million
LinkedIn	2021	700 Million
Yahoo!	2016	3,000 Million

Companies ***Will*** Be Hacked

- We can’t control that
- What does that mean?

Companies ***Will*** Be Hacked

- We can’t control that
- What does that mean?

A Different Password for Each Account

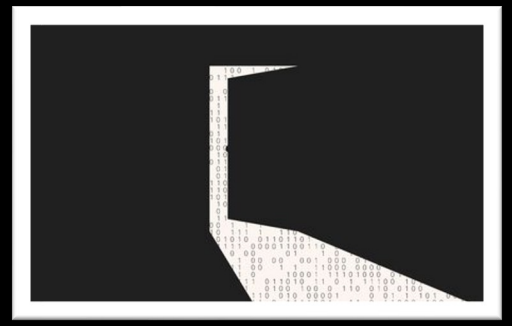
Strong Passwords: Summary

- At least 14 characters
- Include different characters
- Randomly chosen
- Unique

Which Accounts Need $trong Passwords?

- Banking / Finance
- Retailers
- Email

Why Protect Email?

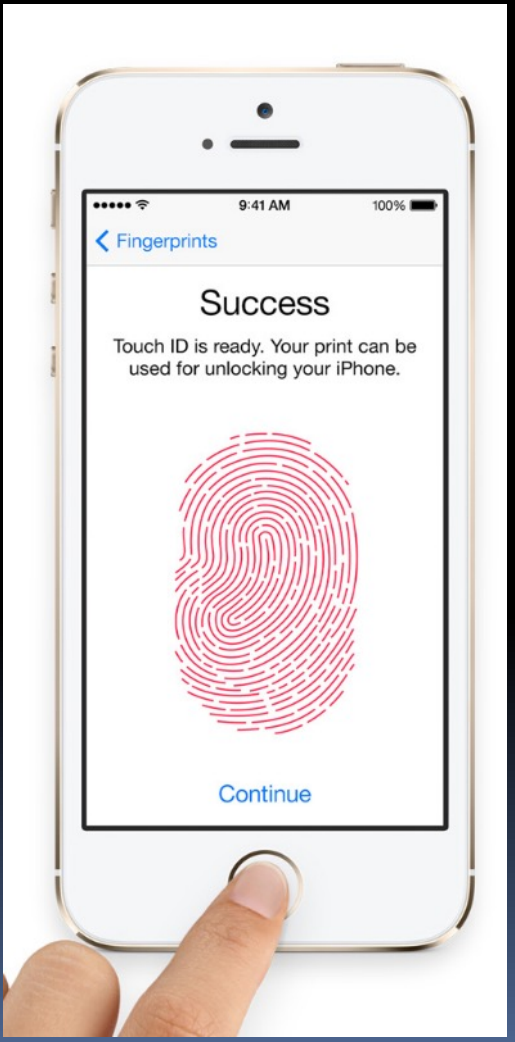


- Email is a backdoor to your accounts
- When you forget a password,
  a password-reset message is sent to you
- If hackers control your email, they can
  reset your password

Anything Easier than Passwords?

Biometric Authentication

- Reads:
  - Fingerprint
  - Face pattern
  - Patterns in eye
  - Voice patterns
- Convenient but secure
- Still need password as backup



1. USE STRONG PASSWORDS

Summary

10 Ways to Protect Yourself Online

10. Use Mobile Devices
9. Use a VPN
8. Use an Ad-Blocker
7. Keep Your Programs Up to Date
6. Use Two-Factor Authentication
5. Be Wary of Social Media
4. Be Suspicious
3. Back Up Your Data
2. Use Password Manager
1. Use Strong Passwords

Rember: Security is as simple as ABC

Always Be Careful