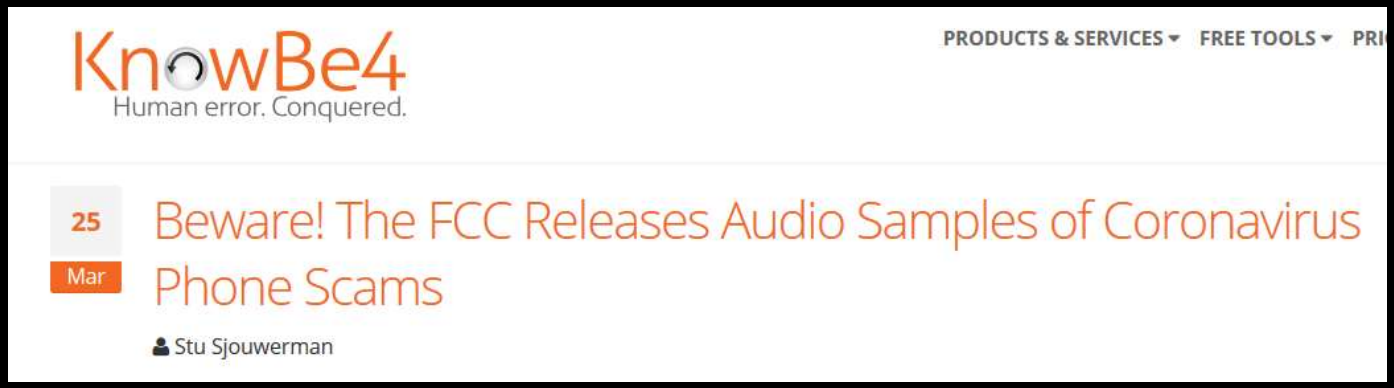

KnowBe4
Human error. Conquered.
PRODUCTS & SERVICES
FREE TOOLS
25
Mar
Beware! The FCC Releases Audio Samples of Coronavirus Phone Scams
Stu Sjouwerman


USA TODAY
Senate lays out who qualifies for $1,200 payments in stimulus bill aimed at helping Am
[News]
Sports
Entertainment
Life
Money
Tech
Travel
Opinion
NATION
Tricksters in white lab coats and phishing emails: Be wary of coronavirus-related scams, officials warn
Jordan Culver USA TODAY
Published 8:22 p.m. ET Mar. 23, 2020 | Updated 12:23 p.m. ET Mar. 24, 2020


LIVE
SHOWS
2020 ELECTIONS
CORONAVIRUS
Coronavirus pandemic creates 'perfect storm' for cybercriminals to exploit people working from home: Experts
Employees unfamiliar with remote work can be particularly vulnerable.

designDATA

WORKING FROM HOME: Cybersecurity Best Practices

Scott Richards | March 26, 2020

designDATA
IT Made Simple. Modern. Secure.

AGENDA

General Cybersecurity Best Practices

Email Security Best Practices

Password Security Best Practices

General Computer Security Tips

designDATA

The Big 4

1. Keep all software, apps, browsers, hardware, etc. on the most current version

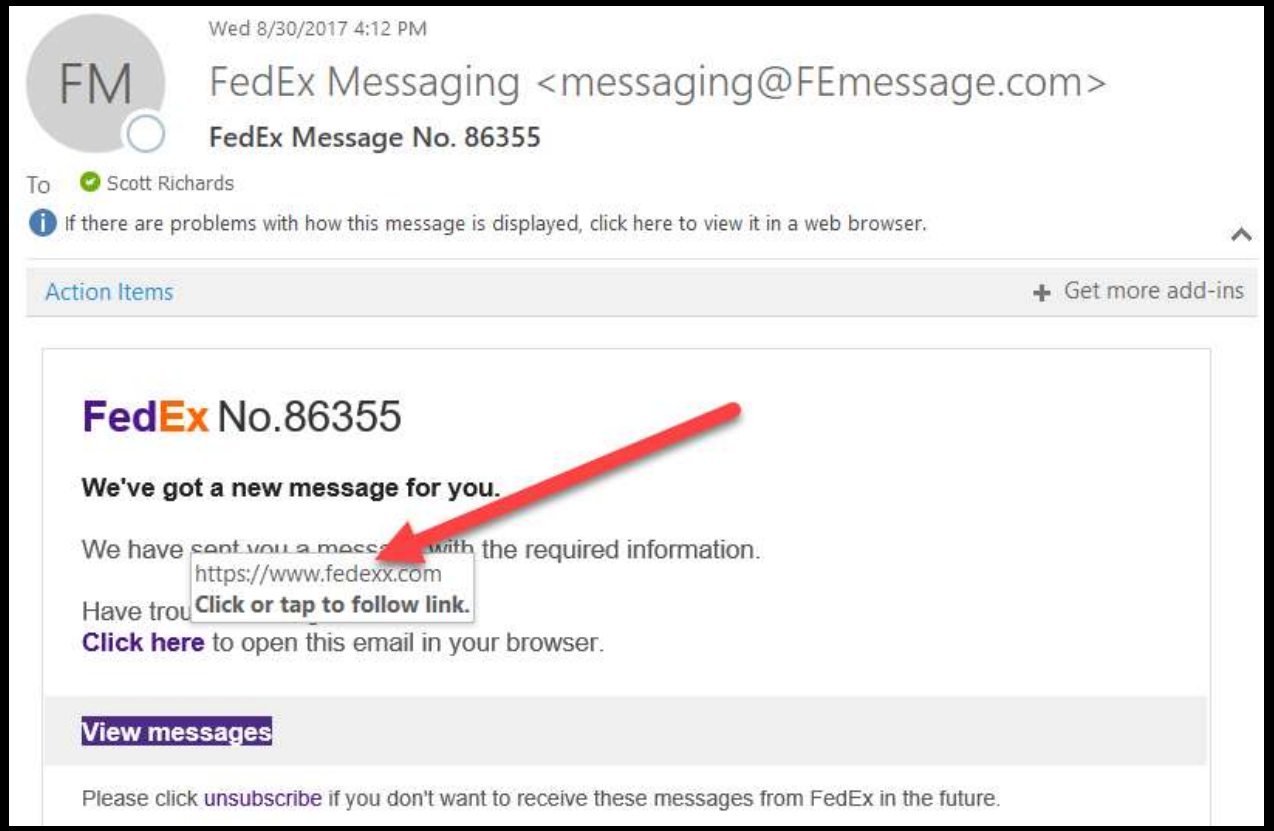
designDATA

The Big 4

2. Back up your files

The Big 4

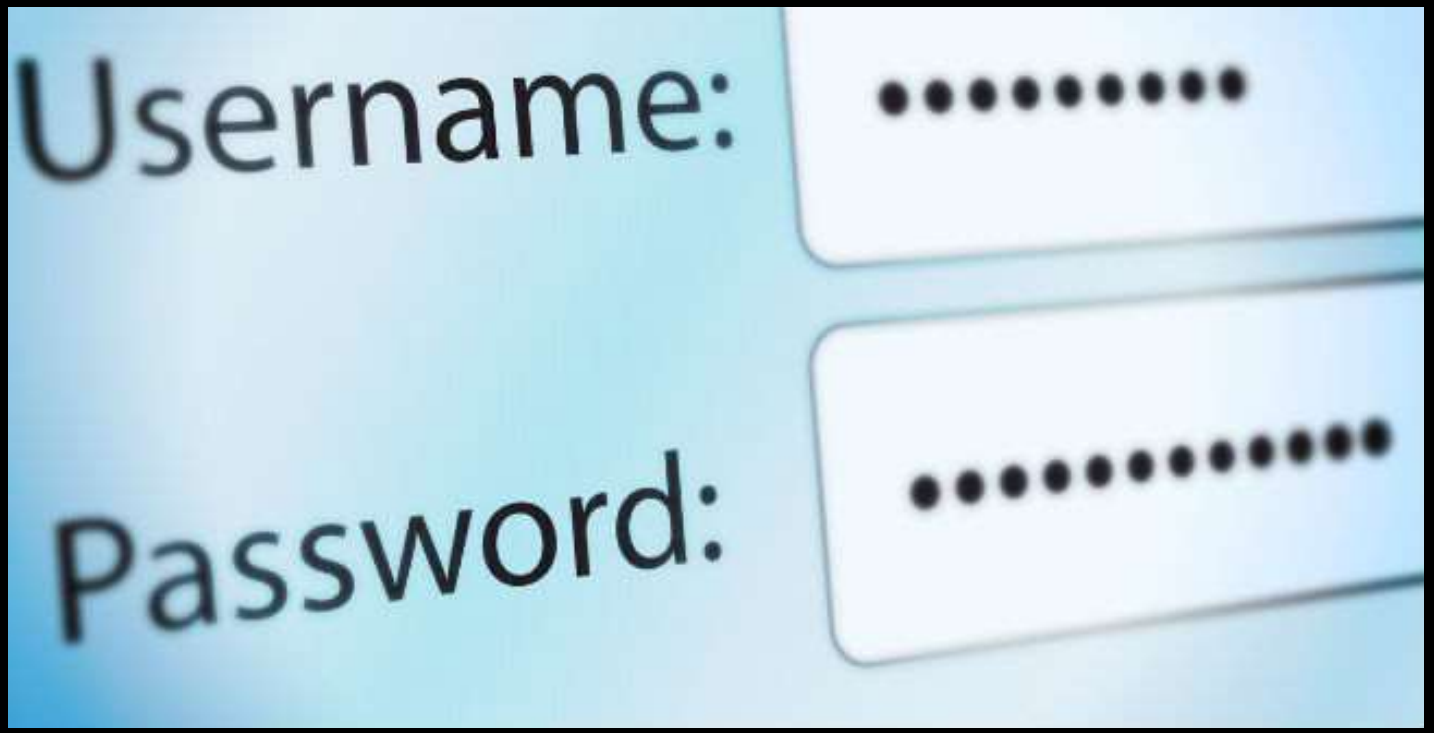
3. Don’t click on links → HOVER!



designDATA

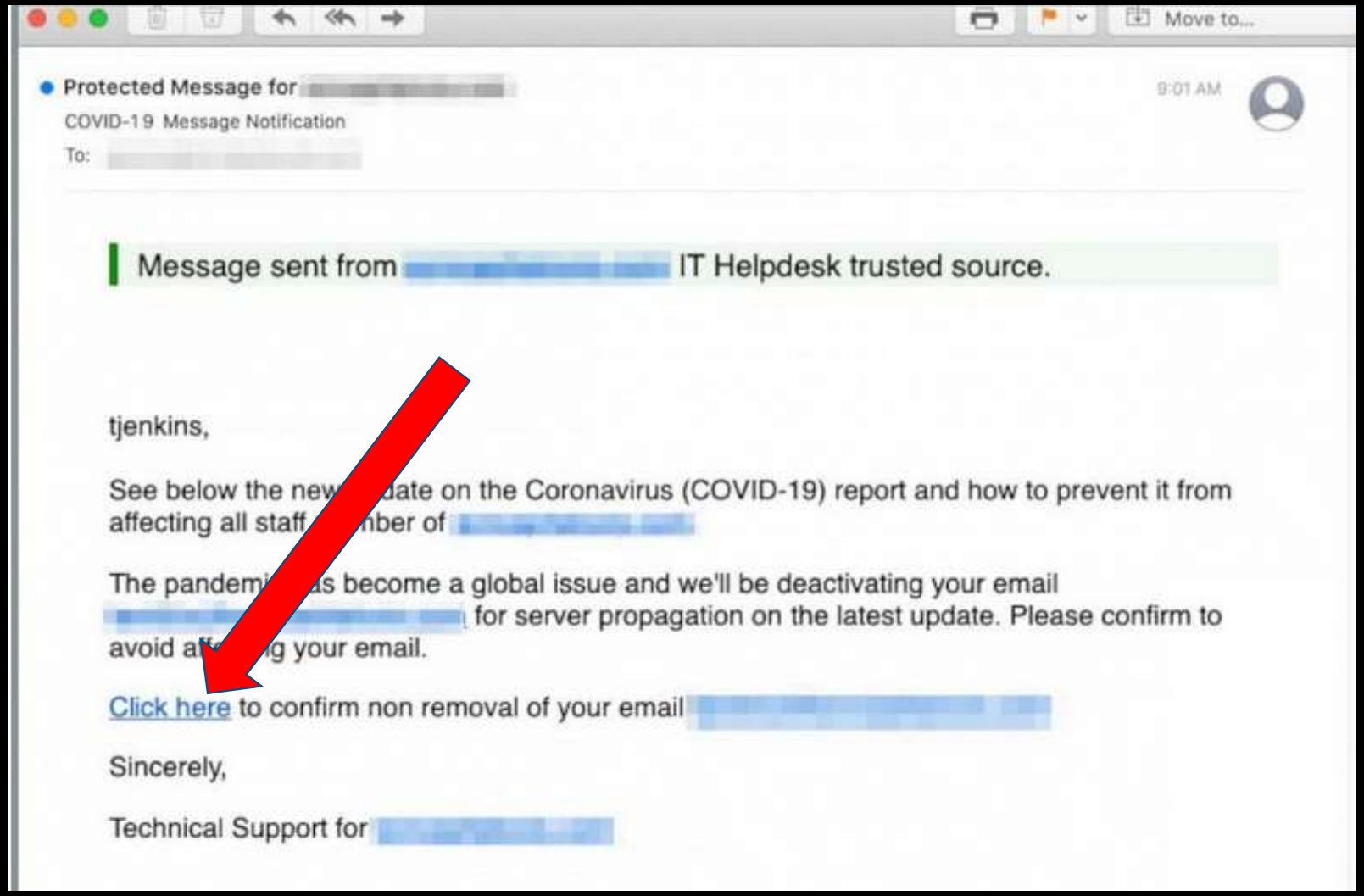
The Big 4

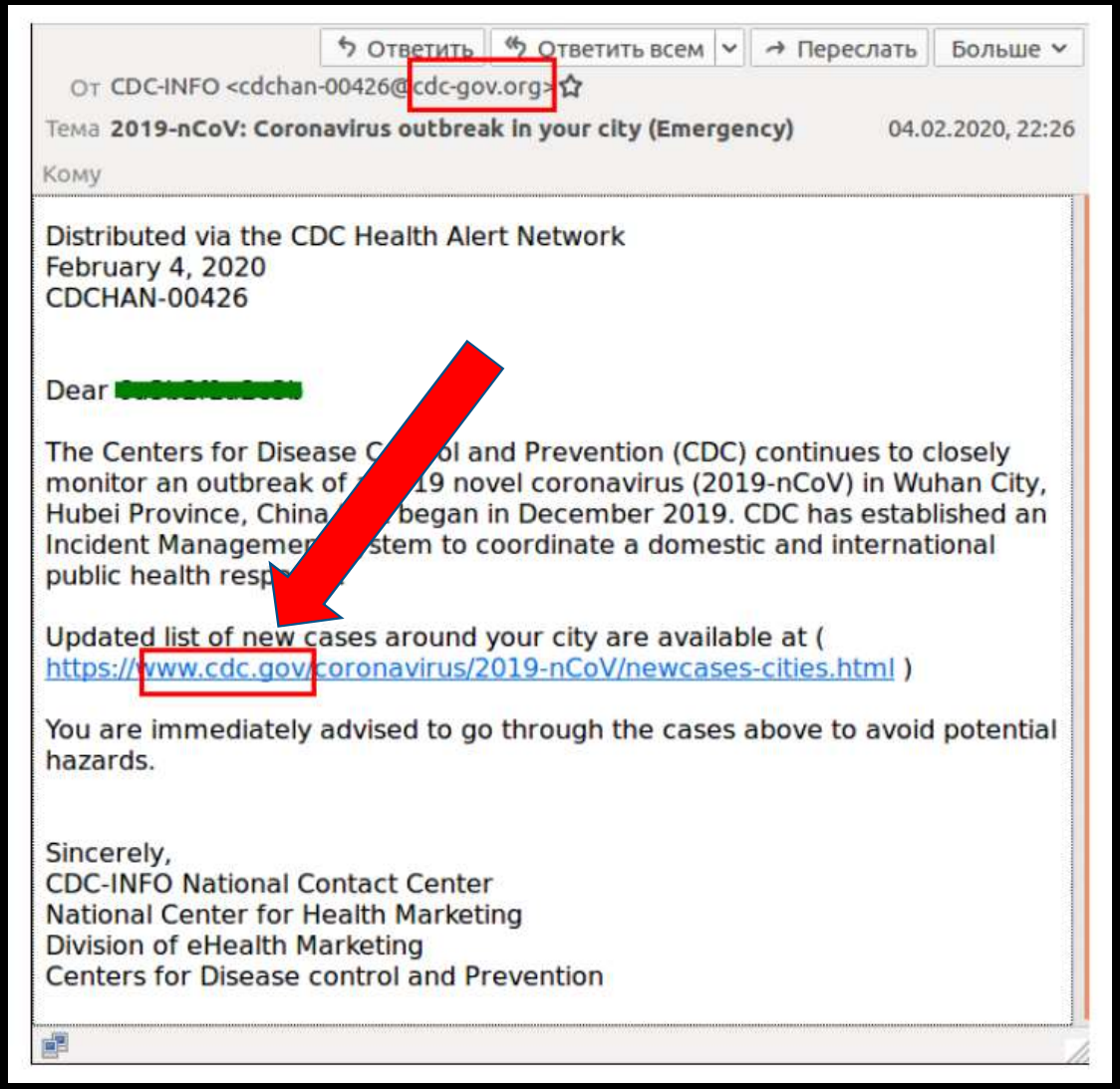
4. Be vigilant with your passwords!

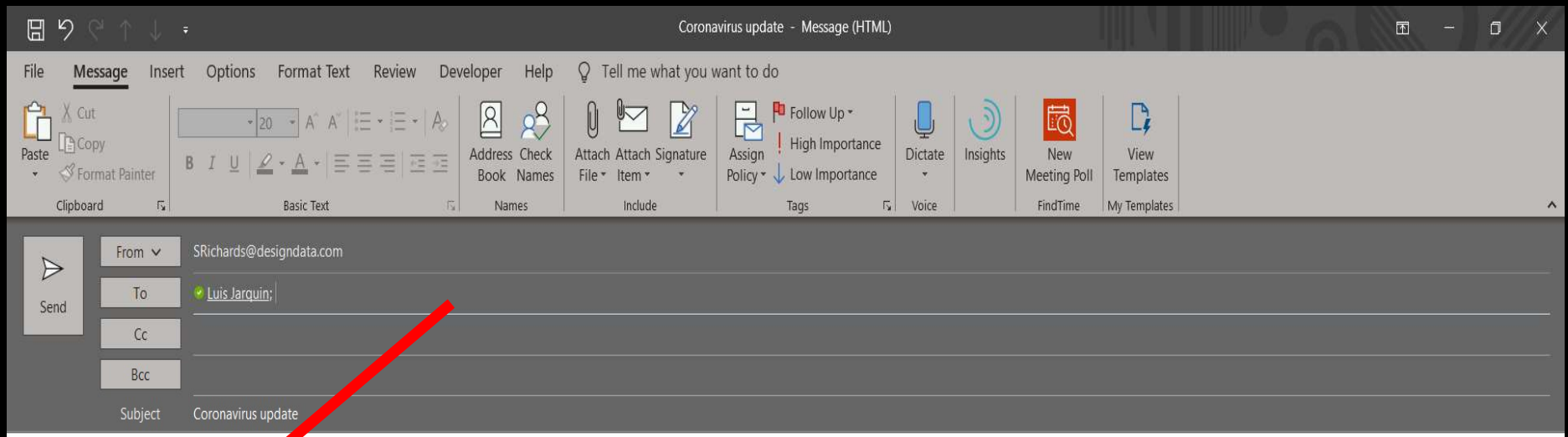


Email Security Best Practices

designDATA

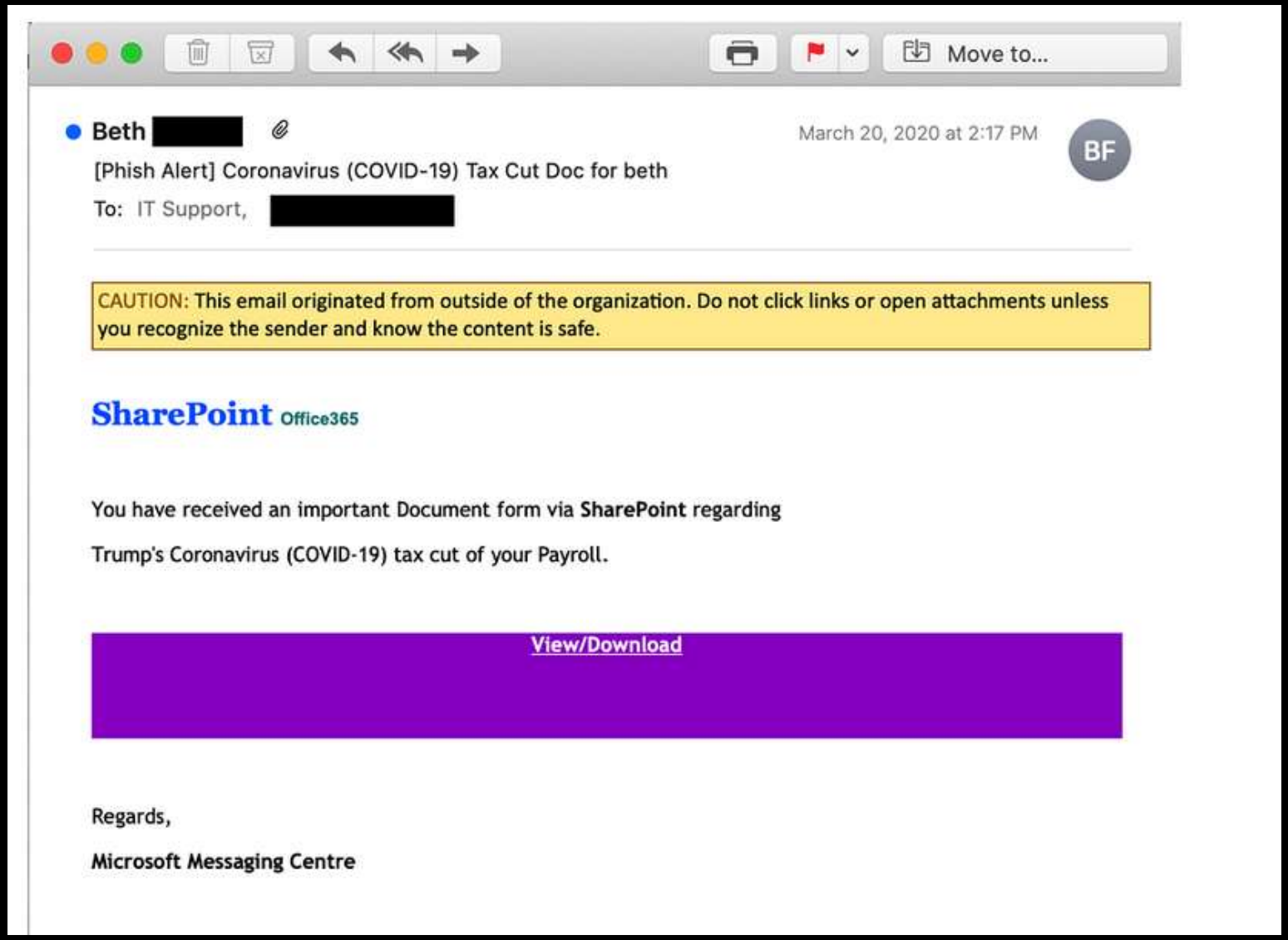

Move to...
Protected Message for
9:01 AM
COVID-19 Message Notification
To:
Message sent from IT Helpdesk trusted source.
tjenkins,
See below the new date on the Coronavirus (COVID-19) report and how to prevent it from affecting all staff nber of
The pandem s become a global issue and we'll be deactivating your email for server propagation on the latest update. Please confirm to avoid a g your email.
Click here to confirm non removal of your email
Sincerely,
Technical Support for


Ответить
Ответить всем
Переслать
Больше
От CDC-INFO <cdchan-00426@cdc-gov.org>
Тема 2019-nCoV: Coronavirus outbreak in your city (Emergency)
04.02.2020, 22:26
Кому
Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426
Dear
The Centers for Disease C ol and Prevention (CDC) continues to closely monitor an outbreak of 19 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China began in December 2019. CDC has established an Incident Managemen stem to coordinate a domestic and international public health resp
Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)
You are immediately advised to go through the cases above to avoid potential hazards.
Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention



The outbreak of Coronavirus is a rapidly developing situation and is likely to affect many travel plans over the coming months. We strongly recommend that anyone travelling or planning to travel takes guidance from the Foreign and Commonwealth office:

https;//eff.org/coronavirus-covid-19-information-for-the-staff


Move to...
Beth [redacted]
March 20, 2020 at 2:17 PM
BF
[Phish Alert] Coronavirus (COVID-19) Tax Cut Doc for beth
To: IT Support, [redacted]
CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
SharePoint Office365
You have received an important Document form via SharePoint regarding
Trump's Coronavirus (COVID-19) tax cut of your Payroll.
View/Download
Regards,
Microsoft Messaging Centre

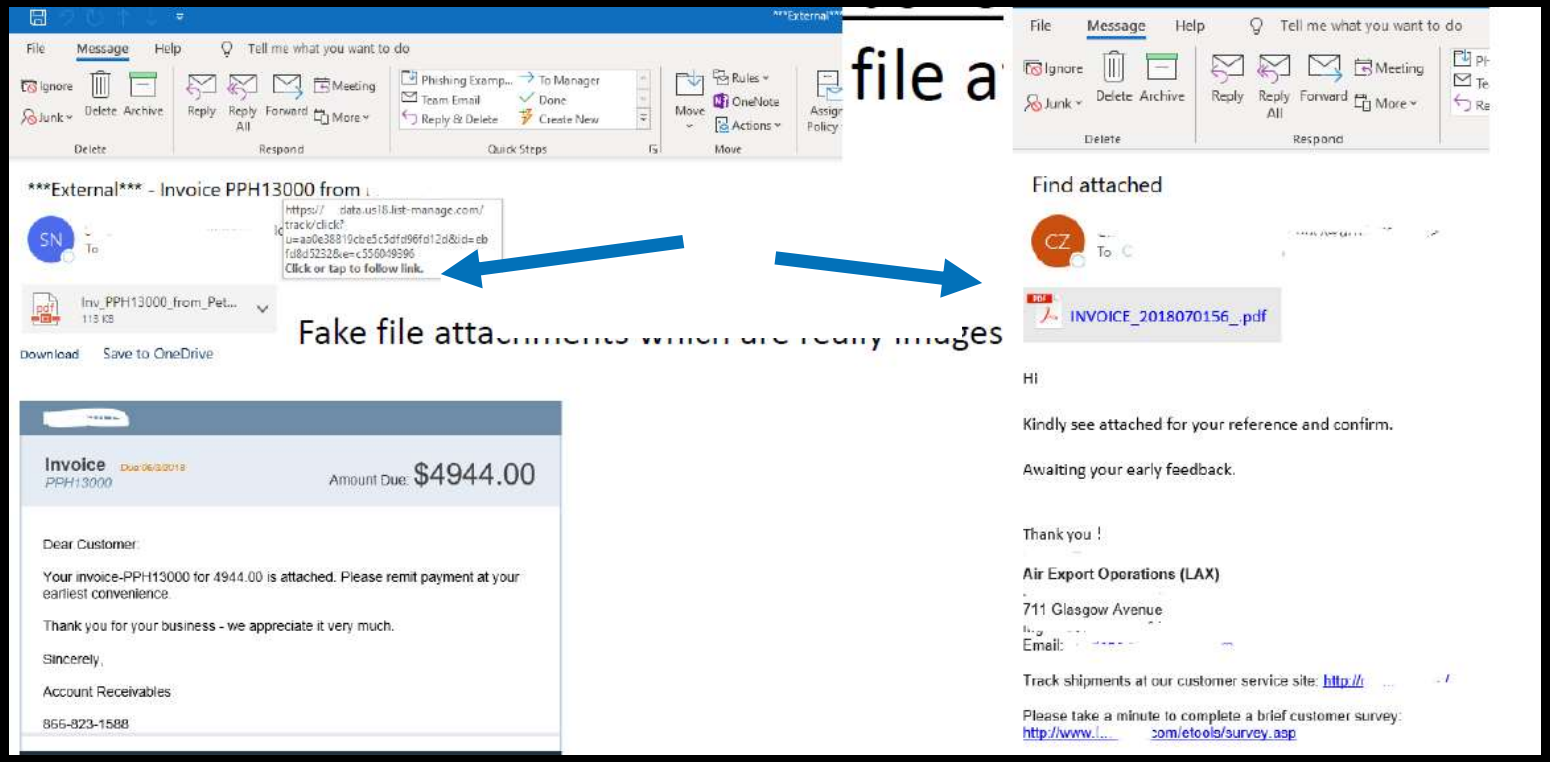
Your dilemma…

How do I know which ones to click on and which ones are dangerous?

DON'T CLICK ON ANYTHING RELATED TO CORONAVIRUS!

1. Go to a trusted web site
2. Turn on the TV or radio

NEW! Fake file attachments that are really images…



designDATA

Hair, anyone?

designDATA

Remember...

“It's not paranoia if they're really out to get you.”

-- Harold Finch, “Person of Interest”

“3 Golden Rules” of Email Security

1. NEVER click on any link until:
   - You’ve **HOVERED** over ALL links to verify they are legitimate
   - You’ve employed the other email “best practices” in this training

2. NEVER click on an attachment until you’ve verified that the email is legitimate
   - See “Email Best Practices” later in this presentation

3. SLOW DOWN and actually READ your emails!

designDATA

Hover, hover, hover!

Let’s take a look!

The consequences…

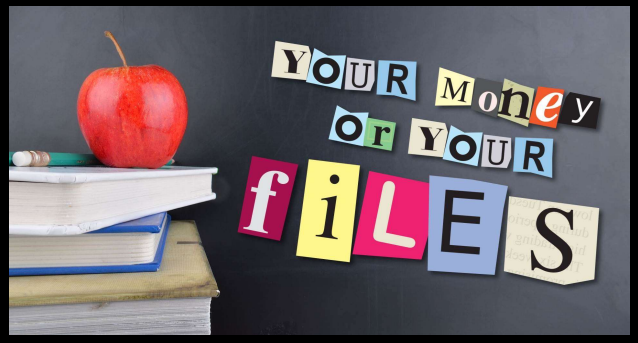
"So what's the worst thing that can happen if I click on one of these Coronavirus links (or any other suspicious links)?"

1. Ransomware

designDATA

Ransomware

- Restricts access to victim's infected computer
- Demands victim pay money to restore access to files
- 40,000 attacks per day
- Takes an average computer 6 trillion years to crack the encryption!



designDATA

Ransomware 2.0 (Feb, 2020)

YOU: “We have a backup of our data, so we’re not paying the ransom!”

HACKER: “OK, no problem. Hope you enjoy having your competitors and the general public see all of your data!”

Imagine every email you and your employees have ever written out there on the Internet!

Coronavirus Mobile Phone Ransomware

- WATCH OUT for Android ransomware posing as a coronavirus update application.
  - Will encrypt and lock the user's phone, demanding Bitcoin in ransom.

2. Keylogger

- Surveillance technology: monitors and records every keystroke
- Used to steal personally identifiable information (PII), login credentials and sensitive enterprise data.

designDATA

How do hackers fool you?

- "Phishing " (aka "Spray and Pray")
  - 156 million phishing emails are sent every day
    - 16 million (10%) get through protection software!

designDATA

Where are Coronavirus phishing emails originating?

- #1 country:

- #2 country:

- Followed by China, India and Russia.

How do hackers fool you?

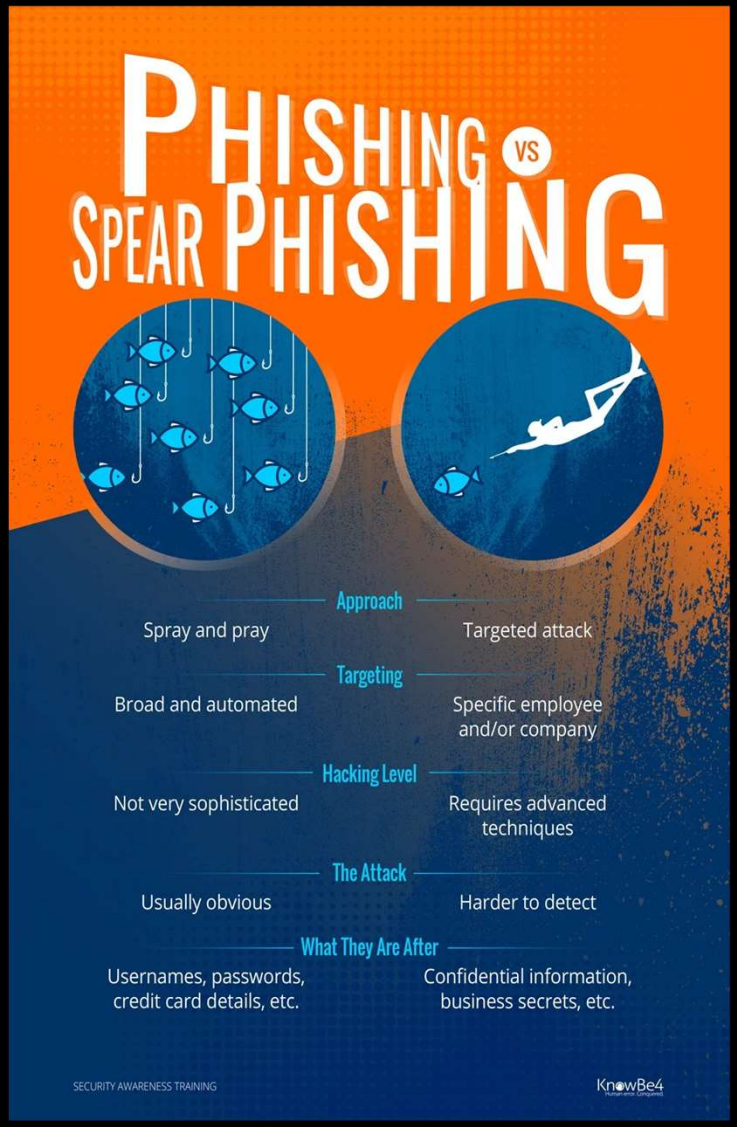
91% of cyber security attacks start with a phishing email!

designDATA

How do hackers fool you?

- "Spear phishing" attack:
  - More targeted type of phishing
  - Perpetrator already knows information about target before making a move
    - Use this info to gain trust

designDATA


PHISHING VS SPEAR PHISHING
Approach
Spray and pray
Targeted attack
Targeting
Broad and automated
Specific employee and/or company
Hacking Level
Not very sophisticated
Requires advanced techniques
The Attack
Usually obvious
Harder to detect
What They Are After
Usernames, passwords, credit card details, etc.
Confidential information, business secrets, etc.
SECURITY AWARENESS TRAINING
KnowBe4

The MASTER spear phishing attack

designDATA

How does your machine get infected?

Two primary ways:

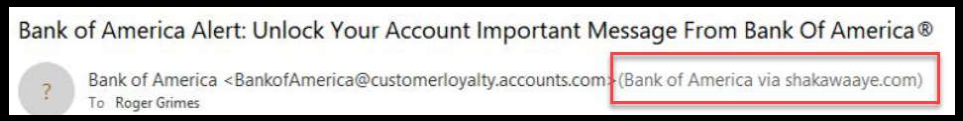
1. **You** open attachments containing the malware
2. **You** click on links that download the malware

designDATA

Email Security Best Practices

ALWAYS:

1. Beware of threatening language
    - e.g. “Click here in the next 24 hours or your account will be deactivated.”
2. Check **“From” and “To”** fields
    - “Disconnected email addresses”



3. Legitimate companies will never ask for personal information via email.
4. Don’t believe everything you see!

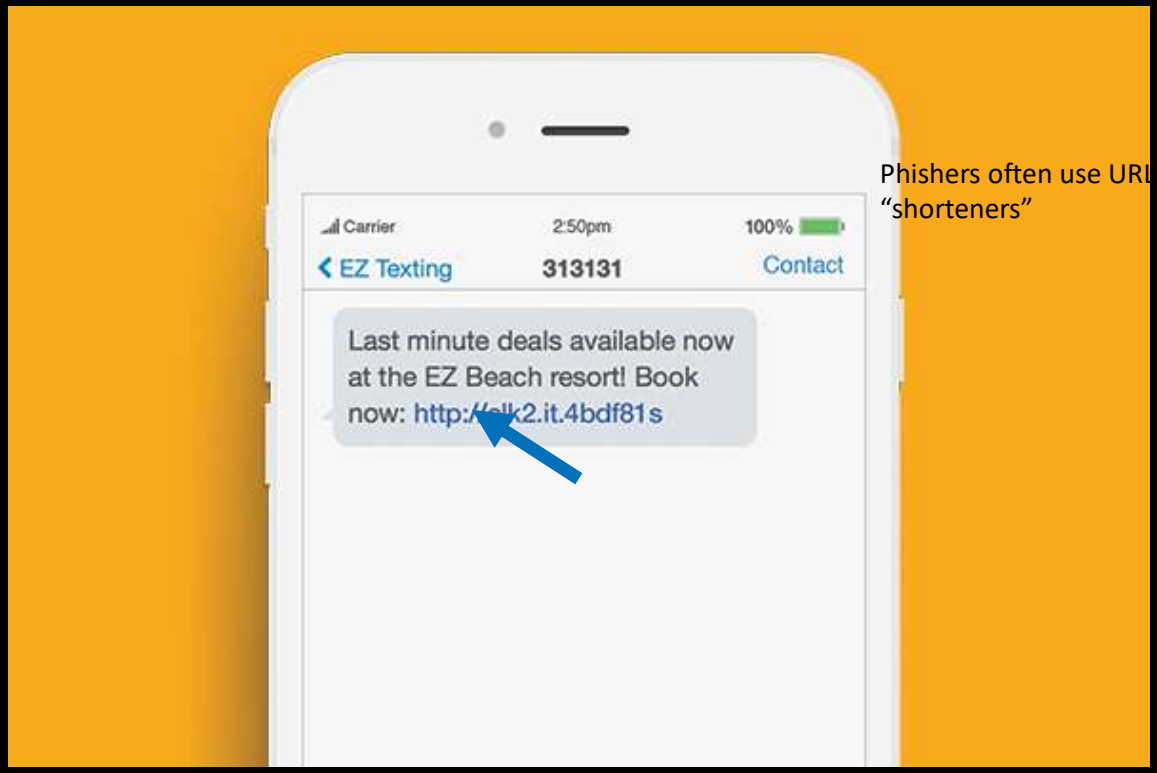
designDATA

Email Security Best Practices

OTHER TIPS:

1. Be careful what you post online!
2. Do not reply to or forward suspicious emails. Either **DELETE**, or contact designDATA for help.
3. Watch out for zeros instead of the letter O; ones instead of the letter “l”
   - G00gle.com
4. Now trending: citìbank.com

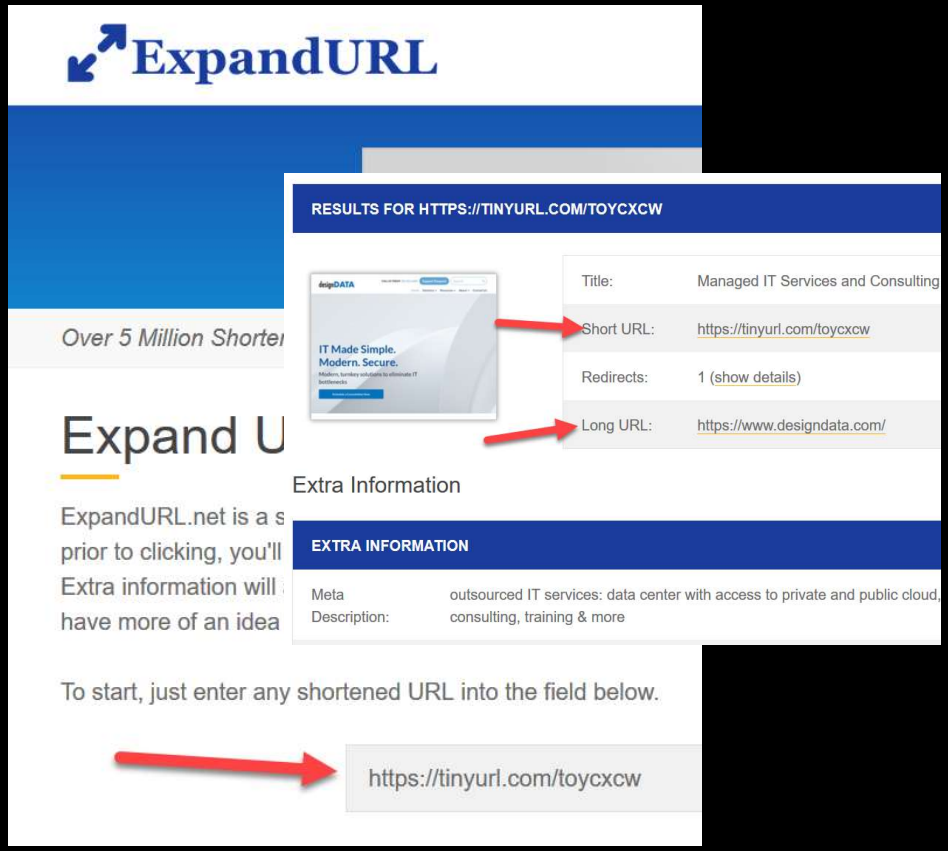
Smishing (SMShing)



Phishers often use URL
"shorteners"

designDATA

URL Expander



designDATA

What to do if…

…you think you are having ANY type of security issue:

Contact the designDATA Service Desk!

designDATA
IT Made Simple. Modern. Secure.

Password Security Best Practices

designDATA

January 15, 2019: Verizon Data Breach Report

81%

of hacking-related breaches
used either stolen or weak passwords.

designDATA

Think your password is safe?

File With 1.4 Billion Hacked And Leaked Passwords Found On The Dark Web

117 million LinkedIn emails and passwords for sale on the Dark Web!

designDATA

The Magic password length

- POLL 1: How long does your password need to be to make it MUCH harder to be hacked?

A. 8 characters
B. 12 characters
C. 15 characters
D. 30 characters

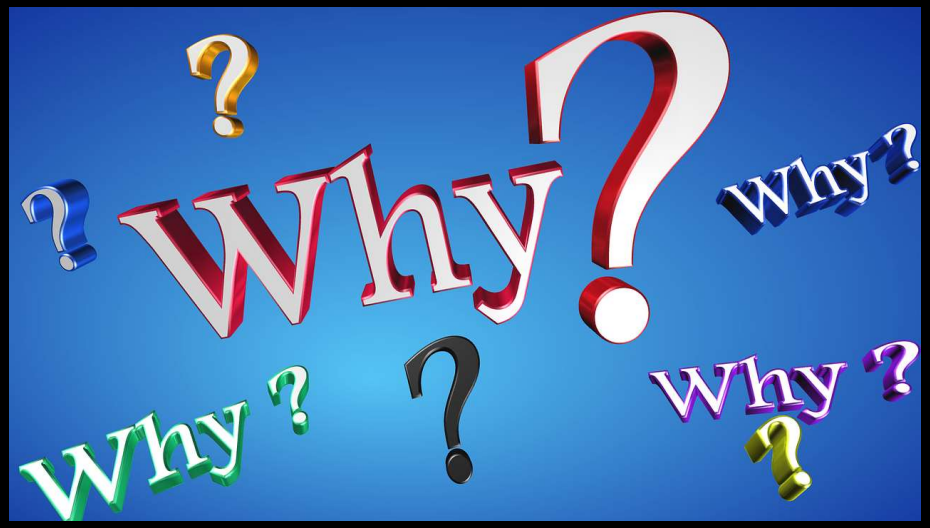
The Magic password length

- POLL 1: How long does your password need to be to make it MUCH harder to be hacked?

A. 8 characters
B. 12 characters
C. 15 characters
D. 30 characters

POLL 2: How many passwords do I need to be safe?

- To be truly safe, you should use a different password for EVERY account.



CNN BUSINESS Markets Tech Media Success Perspectives Videos LIVE TV Edition

A hacker gained access to 100 million Capital One credit card applications and accounts

By Rob McLean, CNN Business

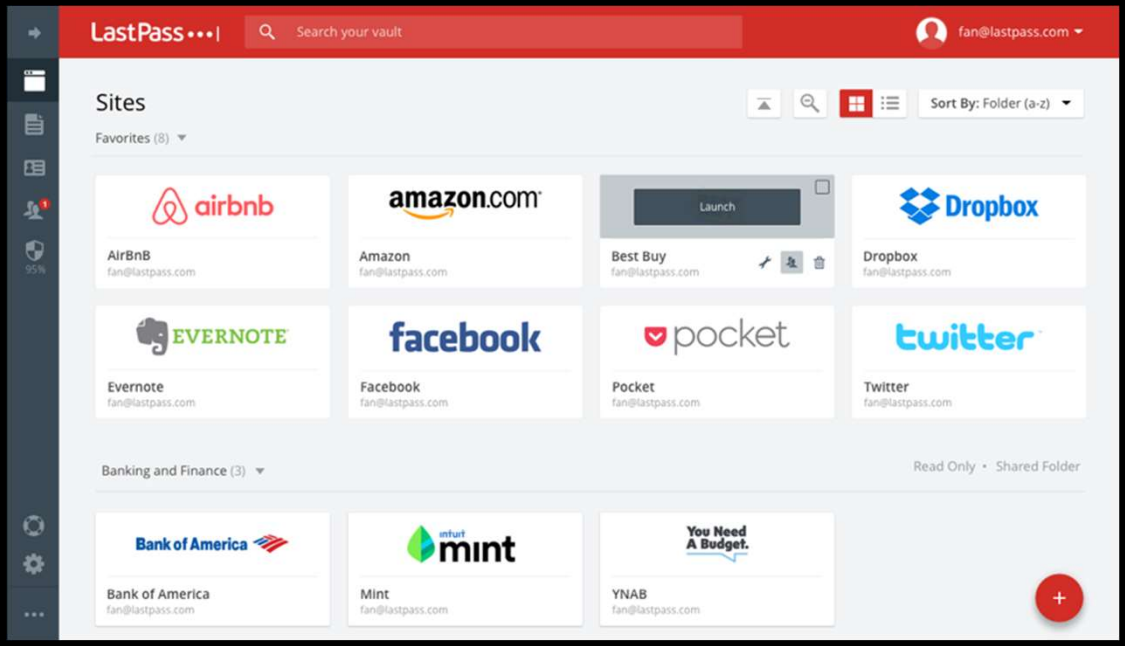
Updated 8:46 AM ET, Tue July 30, 2019

designDATA

So what's the solution?

Password Manager!

- **Unique, complex** passwords for every account
- Don’t have to memorize any passwords!
- Fills in users/passwords for you!



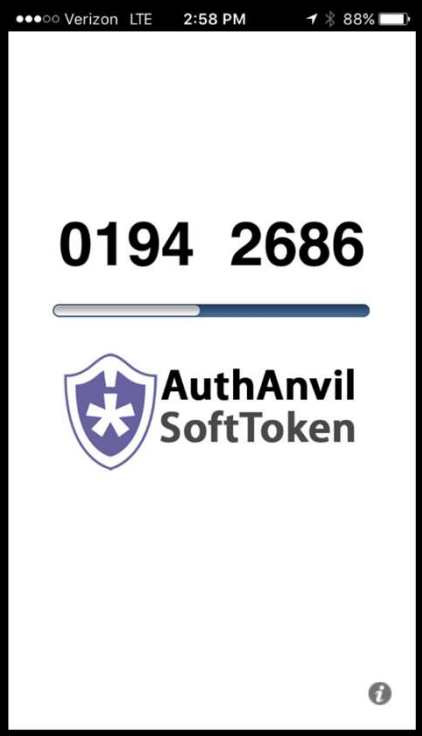
designDATA

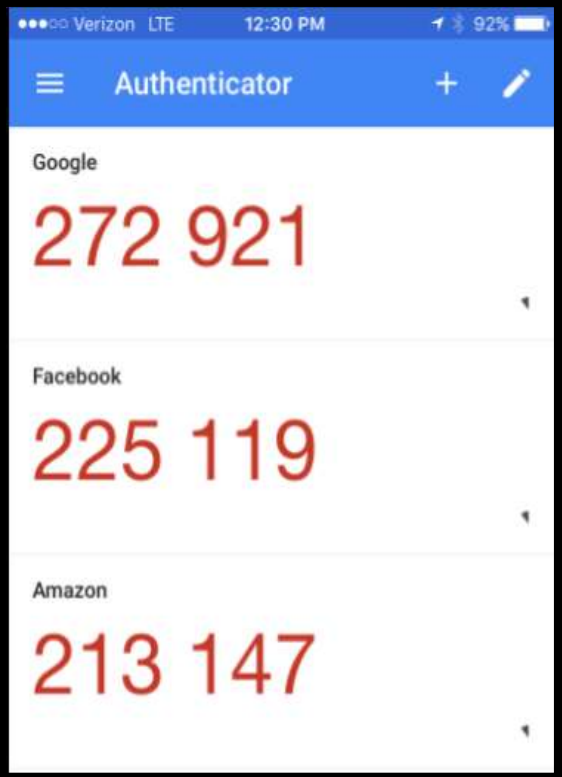
Another great technology: 2 Factor Authentication

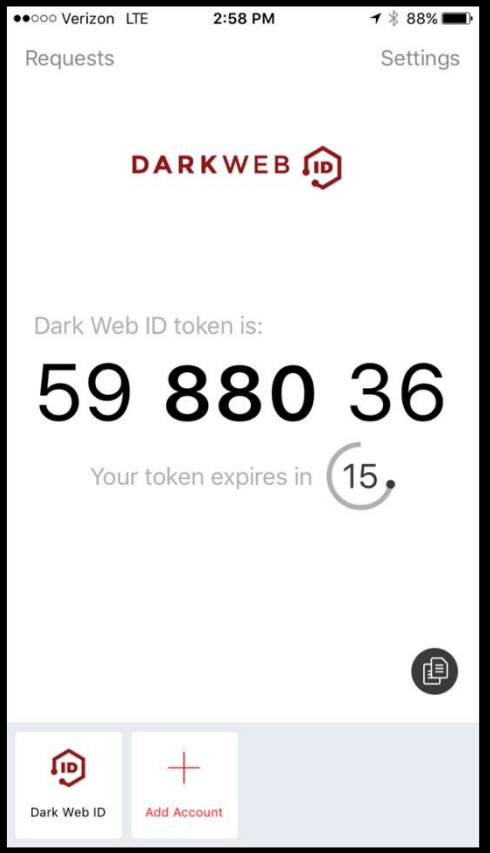
- Need TWO pieces of information to log into an account

designDATA

2 Factor Authentication->Authenticator Apps







designDATA

Let’s take a look!

Password Manager and 2-Factor Authentication

Password Security Best Practices

01	02	03	04	05
 Use a different password for every account	 Use complex passwords	 Use a password manager	 Use 2-factor authentication	 Don't share passwords with other people

designDATA

Key websites

- How secure is your password?
  https://lastpass.com/howsecure.php

- Has your email address been exposed in a data breach?
  https://haveibeenpwned.com/

- Has you password been exposed in a data breach?
  https://haveibeenpwned.com/Passwords