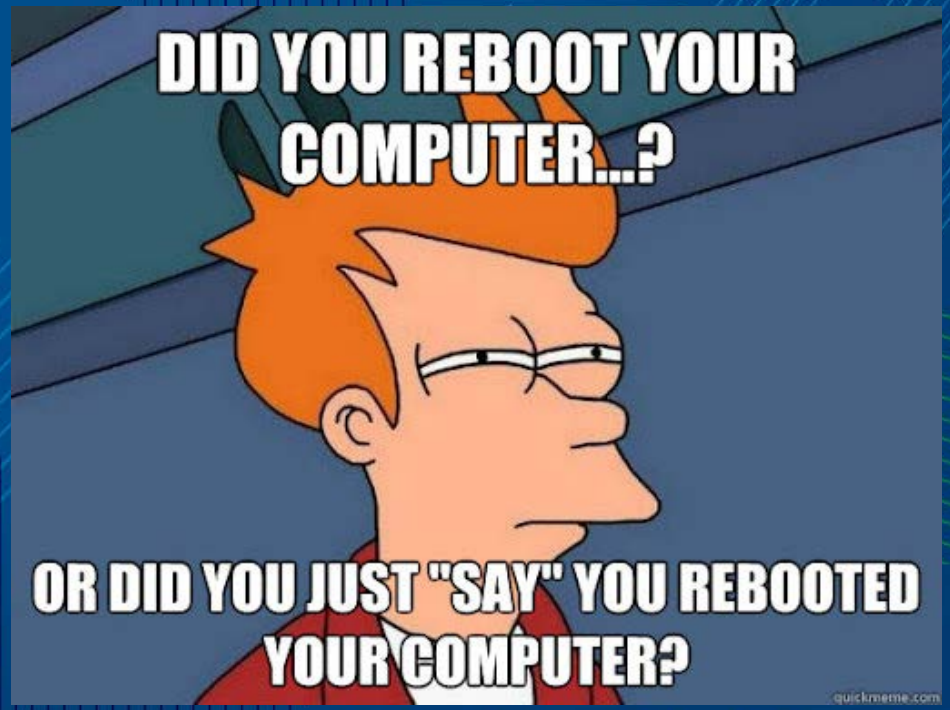
Did you reboot?

Staying secure in the new normal

Marc Vasquez, APR, SACP™

AVP/Security Awareness Program Manager

UMB Financial Corporation



Introduction

As 2021 began, the world faced the possibility that we have not entirely put the unparalleled challenges of 2020 behind us.

Social engineering techniques used by criminally motivated threat actors to tailor phishing campaigns, malicious emails and fraudulent scams are not slowing down.

Introduction

COVID-19 has significantly impacted economic, social, business and political spheres. With the continuing release of vaccines and vaccination rollout plans, financial institutions and social media platforms will likely continue to be the target of intelligence-gathering efforts by state-sponsored adversaries through 2021.

Introduction

When your computer acts up…
When your IT team makes updates…
When you haven't in a while…
When your processors need a break…

Overview

PHISHING

MALWARE

INTERNET OF THINGS

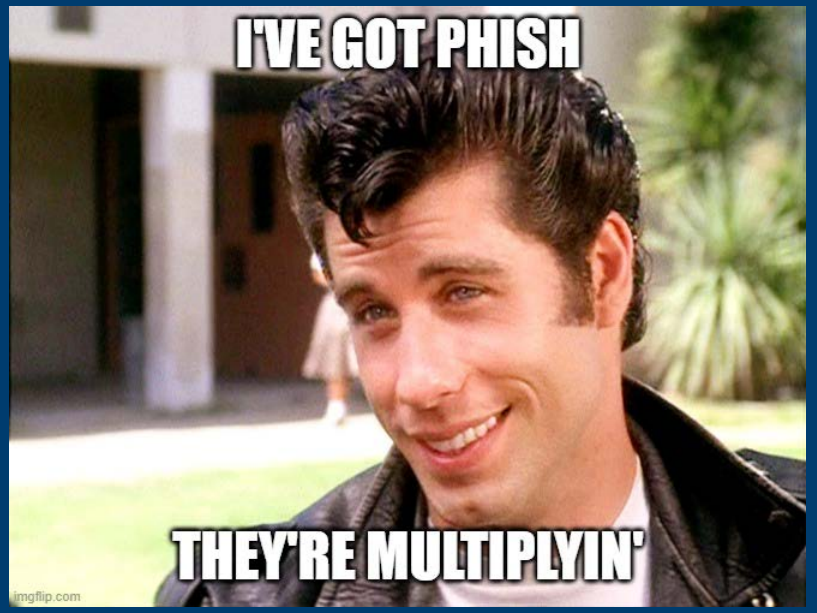
DEEPFAKES AND AI

The new face of social engineering

Phishing

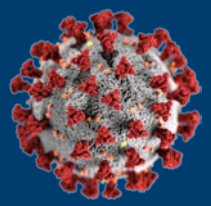
Phishing Activity Trends Report reveals:

- Phishing maintained **near-record levels** in the first quarter of 2021…
- After **landmark increases in 2020** where reported phishing had doubled
- “There are many more attacks that are [going] unreported, meaning that the situation out on the internet **is worse than the mounting numbers** indicate.”



Phishing


FEAR




NEED A JOB!

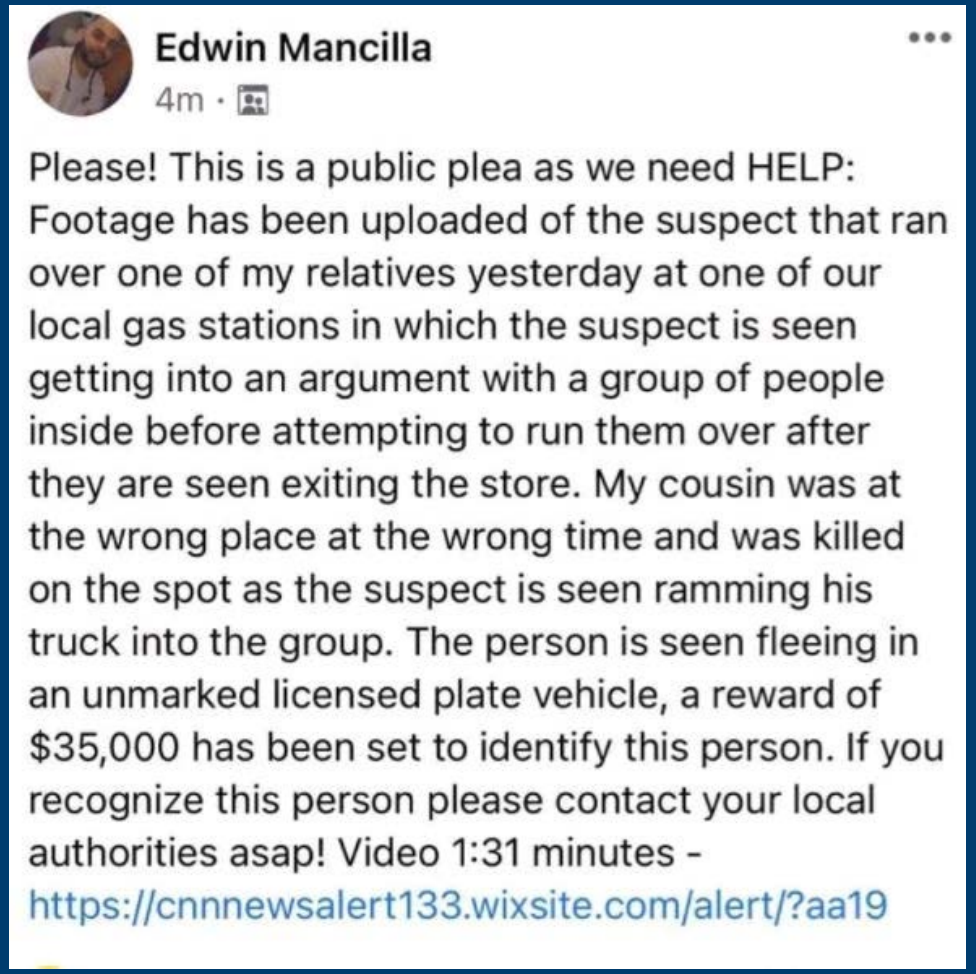

MEMBERS ONLY MONDAYS
FREE COFFEE
MEDIUM • HOT
WITH ANY PURCHASE
FREE
Dunkin' Midnight
Batch
LIMITED BATCH SERIES
DUNKIN'
Original Blend
For Rewards Members only. Limit 1 per member per Monday. Excludes Extra-Charged coffee. Dairy alternatives, espresso shots and flavors may be an additional charge. Participation may vary. Limited time offer.

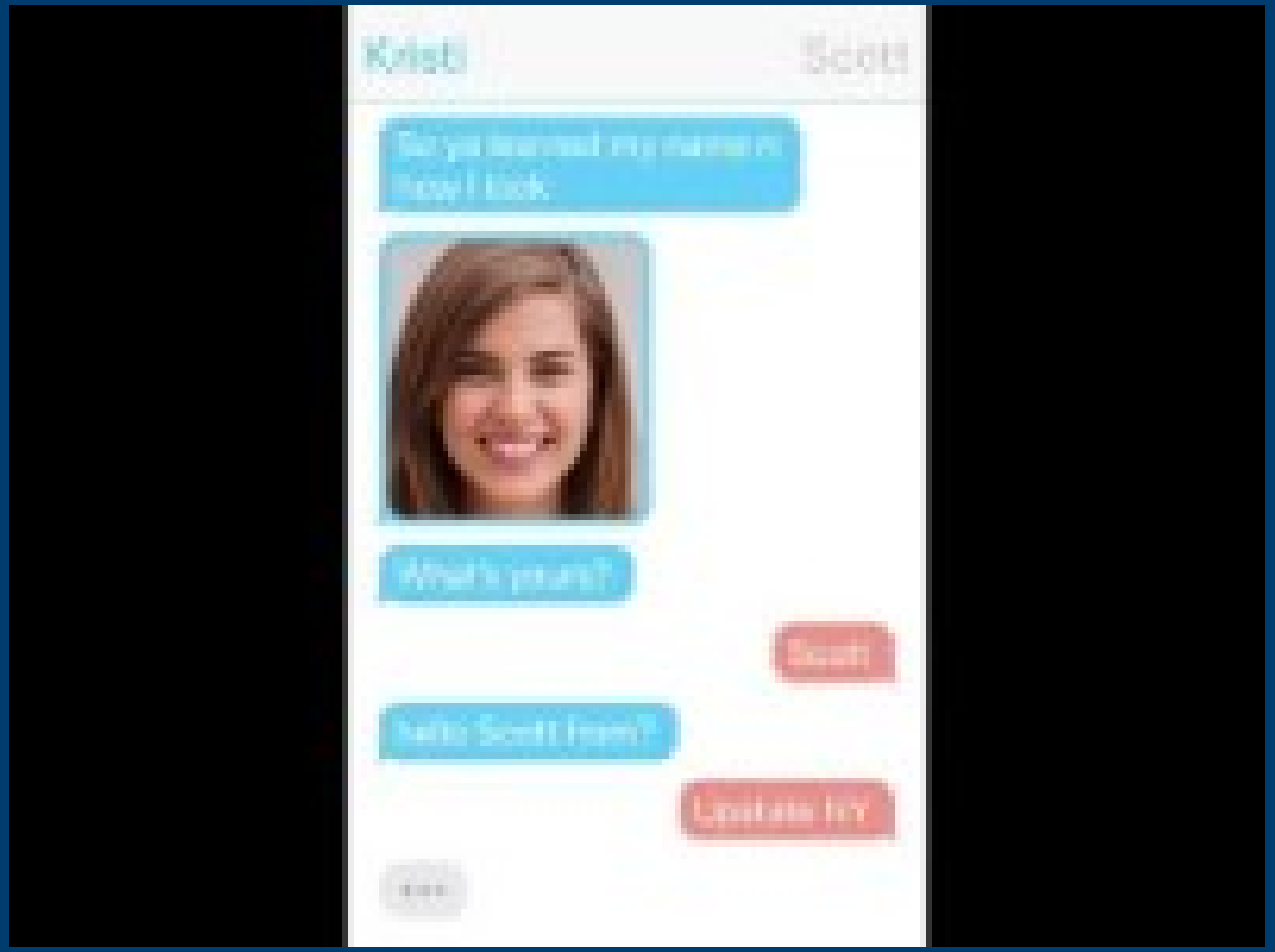

STARBUCKS
COFFEE


VACATION TIME

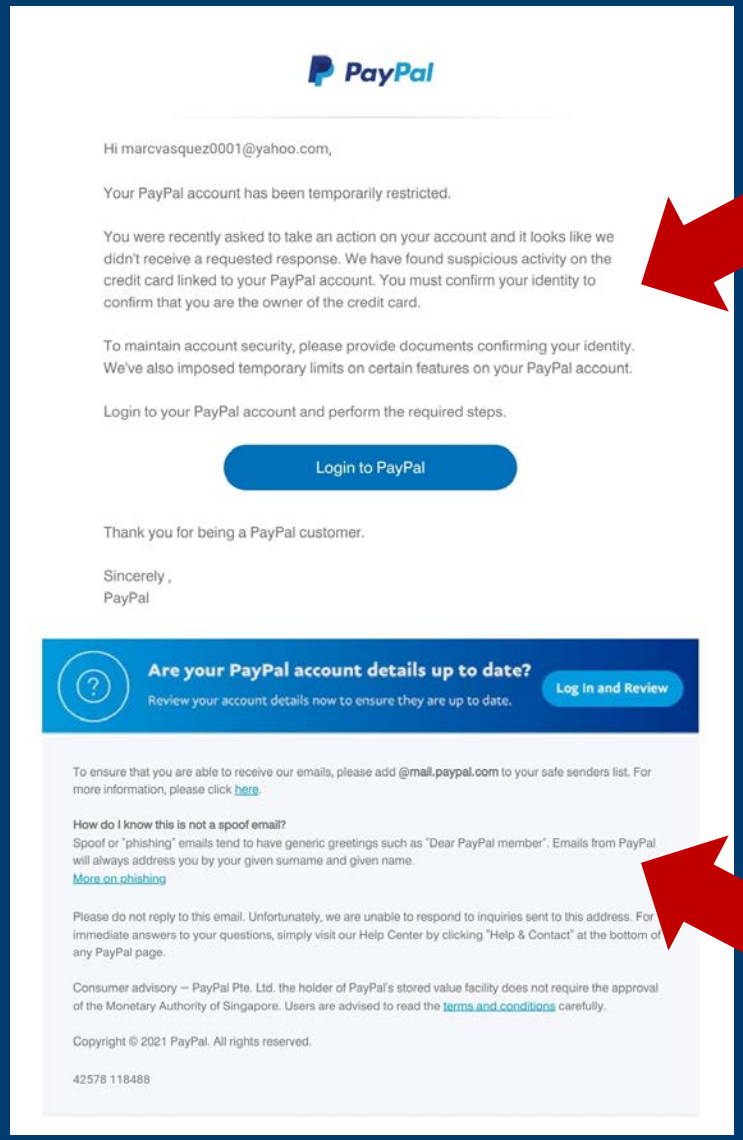

$50

Phishing


Edwin Mancilla
4m ·
Please! This is a public plea as we need HELP: Footage has been uploaded of the suspect that ran over one of my relatives yesterday at one of our local gas stations in which the suspect is seen getting into an argument with a group of people inside before attempting to run them over after they are seen exiting the store. My cousin was at the wrong place at the wrong time and was killed on the spot as the suspect is seen ramming his truck into the group. The person is seen fleeing in an unmarked licensed plate vehicle, a reward of $35,000 has been set to identify this person. If you recognize this person please contact your local authorities asap! Video 1:31 minutes - https://cnnnewsalert133.wixsite.com/alert/?aa19



Phishing



PayPal

Hi marcvasquez0001@yahoo.com,

Your PayPal account has been temporarily restricted.

You were recently asked to take an action on your account and it looks like we didn't receive a requested response. We have found suspicious activity on the credit card linked to your PayPal account. You must confirm your identity to confirm that you are the owner of the credit card.

To maintain account security, please provide documents confirming your identity. We've also imposed temporary limits on certain features on your PayPal account.

Login to your PayPal account and perform the required steps.

Login to PayPal

Thank you for being a PayPal customer.

Sincerely ,
PayPal

Are your PayPal account details up to date?
Review your account details now to ensure they are up to date.
Log In and Review

To ensure that you are able to receive our emails, please add @mail.paypal.com to your safe senders list. For more information, please click here.

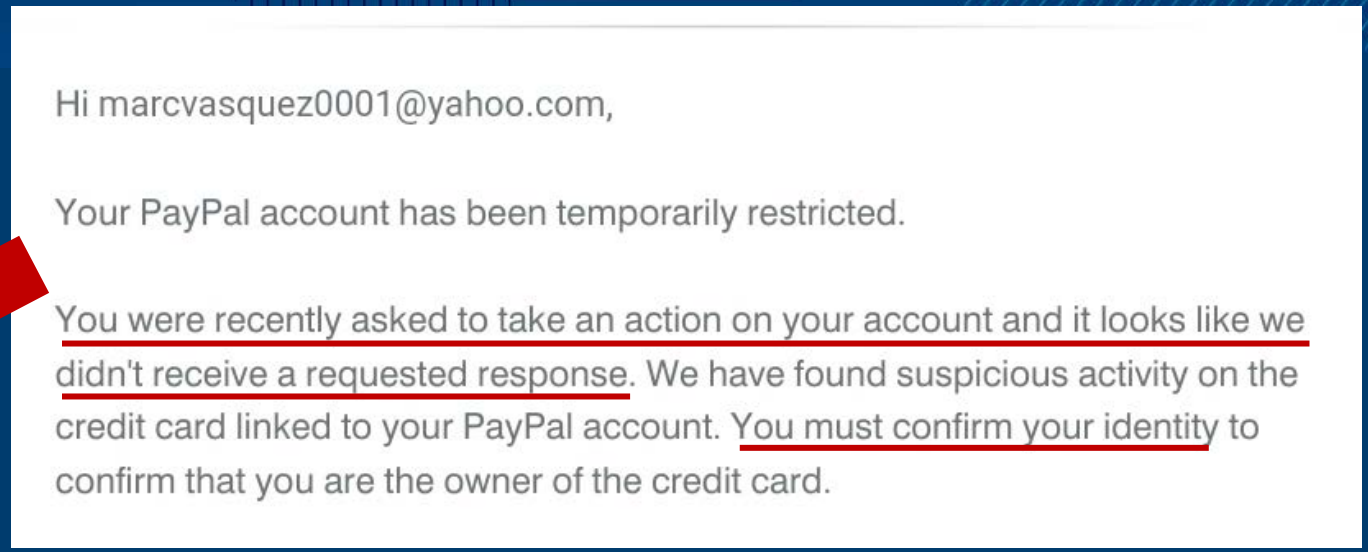
How do I know this is not a spoof email?
Spoof or "phishing" emails tend to have generic greetings such as "Dear PayPal member". Emails from PayPal will always address you by your given surname and given name.
More on phishing

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help & Contact" at the bottom of any PayPal page.

Consumer advisory – PayPal Pte. Ltd. the holder of PayPal's stored value facility does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully.

Copyright © 2021 PayPal. All rights reserved.

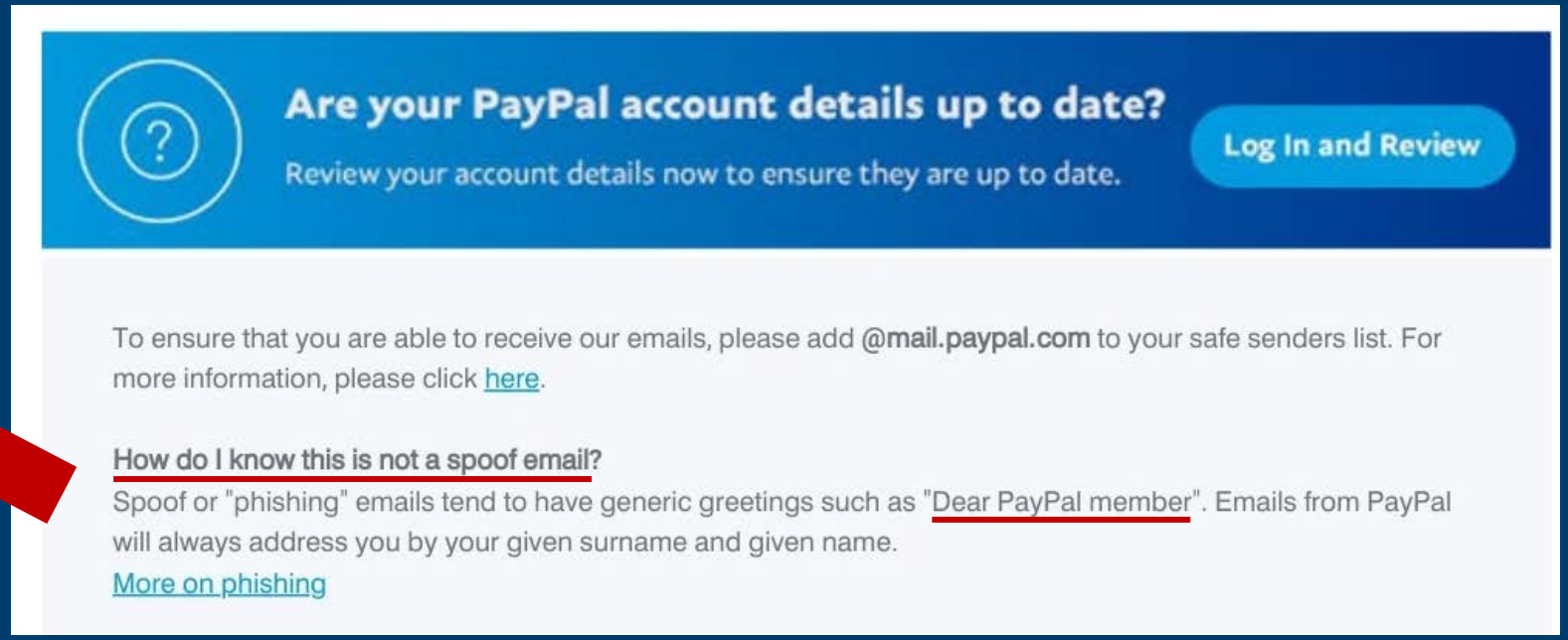
42578 118488



Hi marcvasquez0001@yahoo.com,

Your PayPal account has been temporarily restricted.

You were recently asked to take an action on your account and it looks like we didn't receive a requested response. We have found suspicious activity on the credit card linked to your PayPal account. You must confirm your identity to confirm that you are the owner of the credit card.

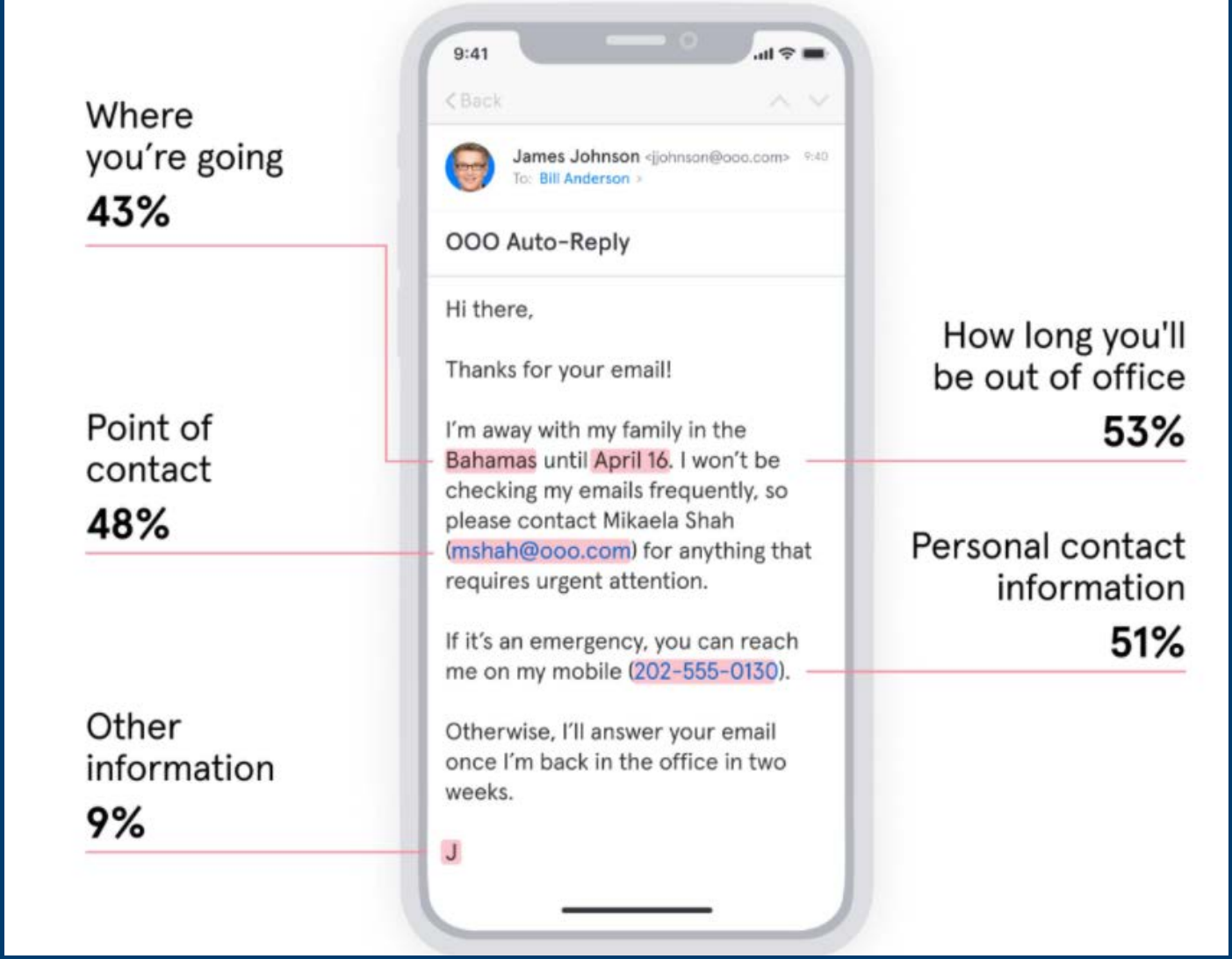


Are your PayPal account details up to date?
Review your account details now to ensure they are up to date.
Log In and Review

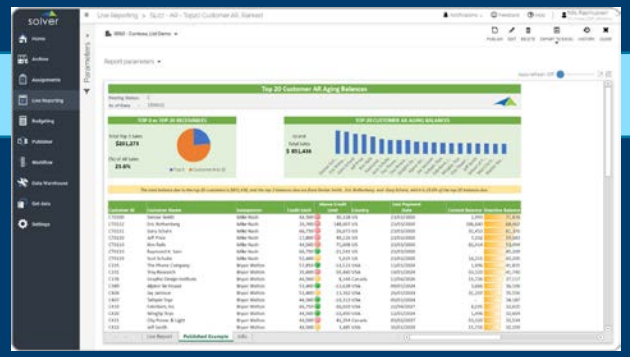
To ensure that you are able to receive our emails, please add @mail.paypal.com to your safe senders list. For more information, please click here.

How do I know this is not a spoof email?
Spoof or "phishing" emails tend to have generic greetings such as "Dear PayPal member". Emails from PayPal will always address you by your given surname and given name.
More on phishing

Phishing


Where you're going
43%
Point of contact
48%
Other information
9%
9:41
Back
James Johnson <jjohnson@ooo.com> 9:40
To: Bill Anderson
OOO Auto-Reply
Hi there,
Thanks for your email!
I'm away with my family in the Bahamas until April 16. I won't be checking my emails frequently, so please contact Mikaela Shah (mshah@ooo.com) for anything that requires urgent attention.
If it's an emergency, you can reach me on my mobile (202-555-0130).
Otherwise, I'll answer your email once I'm back in the office in two weeks.
J
How long you'll be out of office
53%
Personal contact information
51%

Phishing – Business Email Compromise

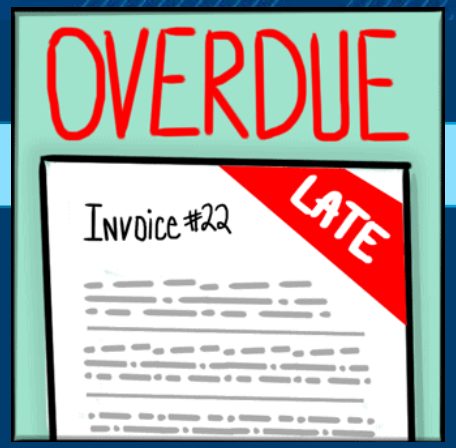


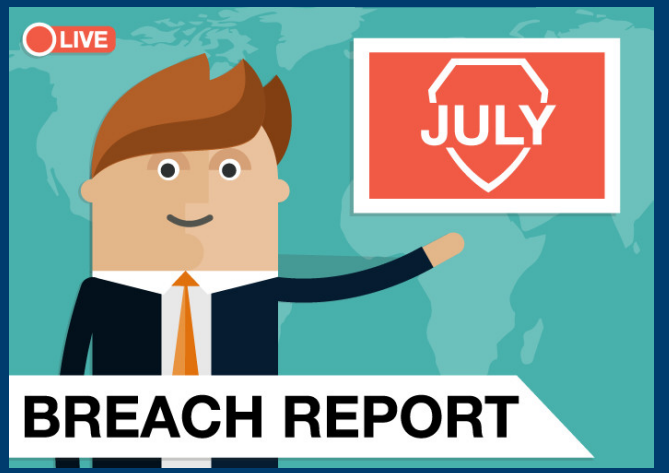
OCEANVIEW, INC. - CLIENT

CONTACTS

SETUP | YOUR DATA

Customer ID	Company	Contact	Contact Type
CU0001	Adventure Works	Greg Akselrod	Personal
CU0002	A Datum Corporat	Abolrous, Hazem	Business
CU0003	Alpine Ski House	Abu-Deyah, Ahmed	Personal
CU0004	Blue Yonder Airlin	Ackerman, Pilar	Business
CU0005	City Power & Light	Adams, Terry	Business
CU0006	Coho Vineyard	Agarwal, Nupur	Business
CU0007	Coho Winery	Alexander, Sean P	Business
CU0008	Coho Vineyard & V	Barnett, Dave	Business



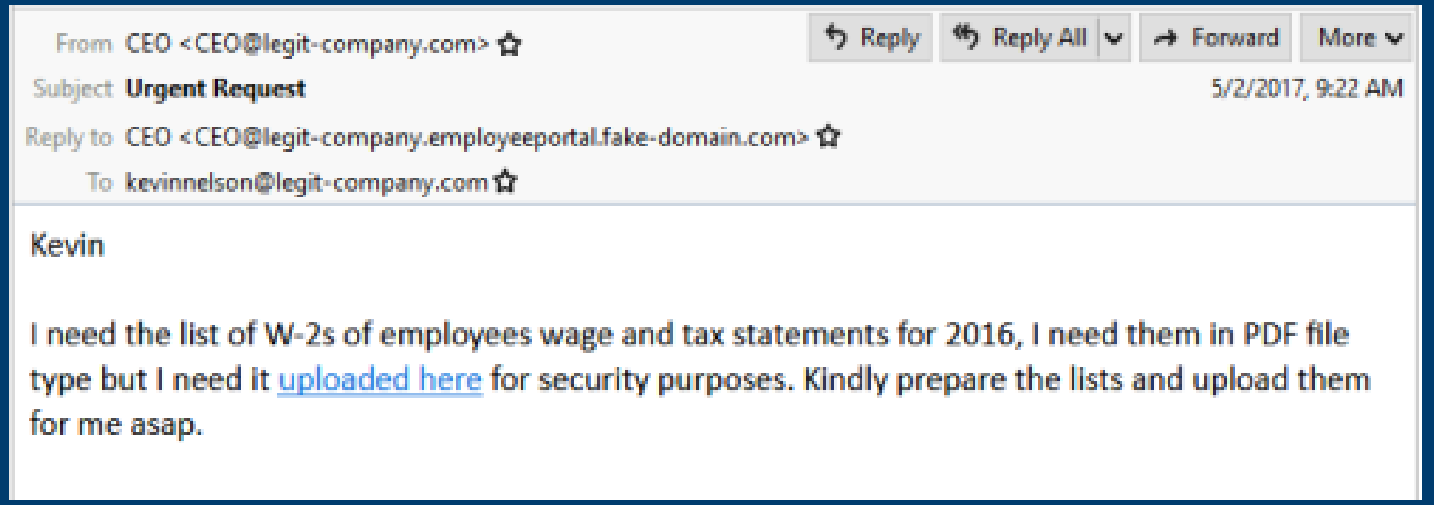


Phishing – Business Email Compromise

Between May 2020 and June 2021, security researchers analyzed:

- More than 12 million spear phishing and social engineering attacks
- The impact on more than 3 million mailboxes
- Covering more than 17,000 organizations

They found that **one in 10 social engineering attacks** are business email compromises (BEC).



Malware

Ransomware/malware is the threat of 2021

- Security researchers have even discovered that ransomware attacks against **healthcare** have jumped about 45 percent since early November 2020.
- In addition, 69 percent of **financial institutions** had been victims of cyberattacks (PPP).

Malware

CovidLock:

- This type of ransomware infects victims via malicious files promising to offer more information about COVID-19
- Once installed, CovidLock encrypts data from devices and denies access. To be granted access, you must pay a ransom of USD 100 per device

Malware

“Smaller organization”:

- When a team member leaves whether due to a new job offer, changes of circumstance, illness or in unfortunate cases, death, that account should be removed from corporate networks
- This oversight is one that cybercriminals took advantage of to exploit more than 100 account in order to spread ransomware

> *All of your files have been encrypted with military grade algorithms. We ensure that the only way to retrieve your data is with our software. We will make sure that you receive your data swiftly and securely when our demands are met. Restoration of your data requires a private key which only we possess. A large amount of your private files have been extracted and is kept in a secure location. If you do not contact us in seven working days of the breach we will start leaking the data. After you contact us we will provide you proof that your files has been extracted. To confirm that our decryption software works email to us two files from random computers. You will receive further instructions after you send us the test files.*

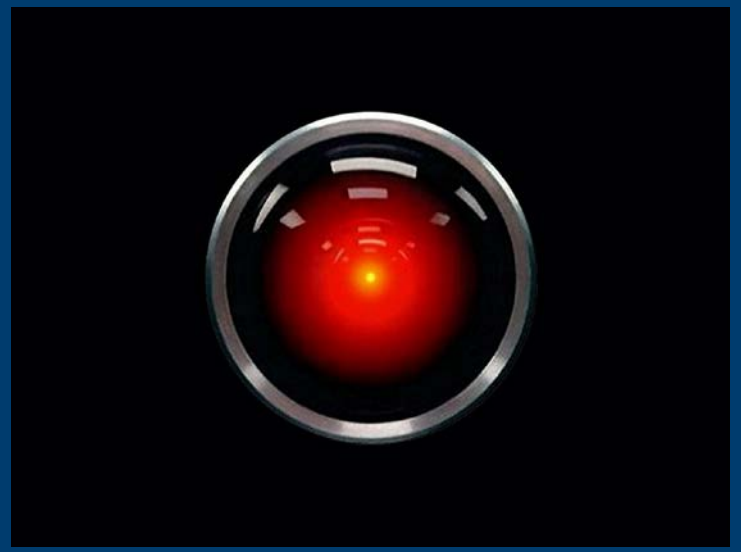
Internet of things

Internet of things

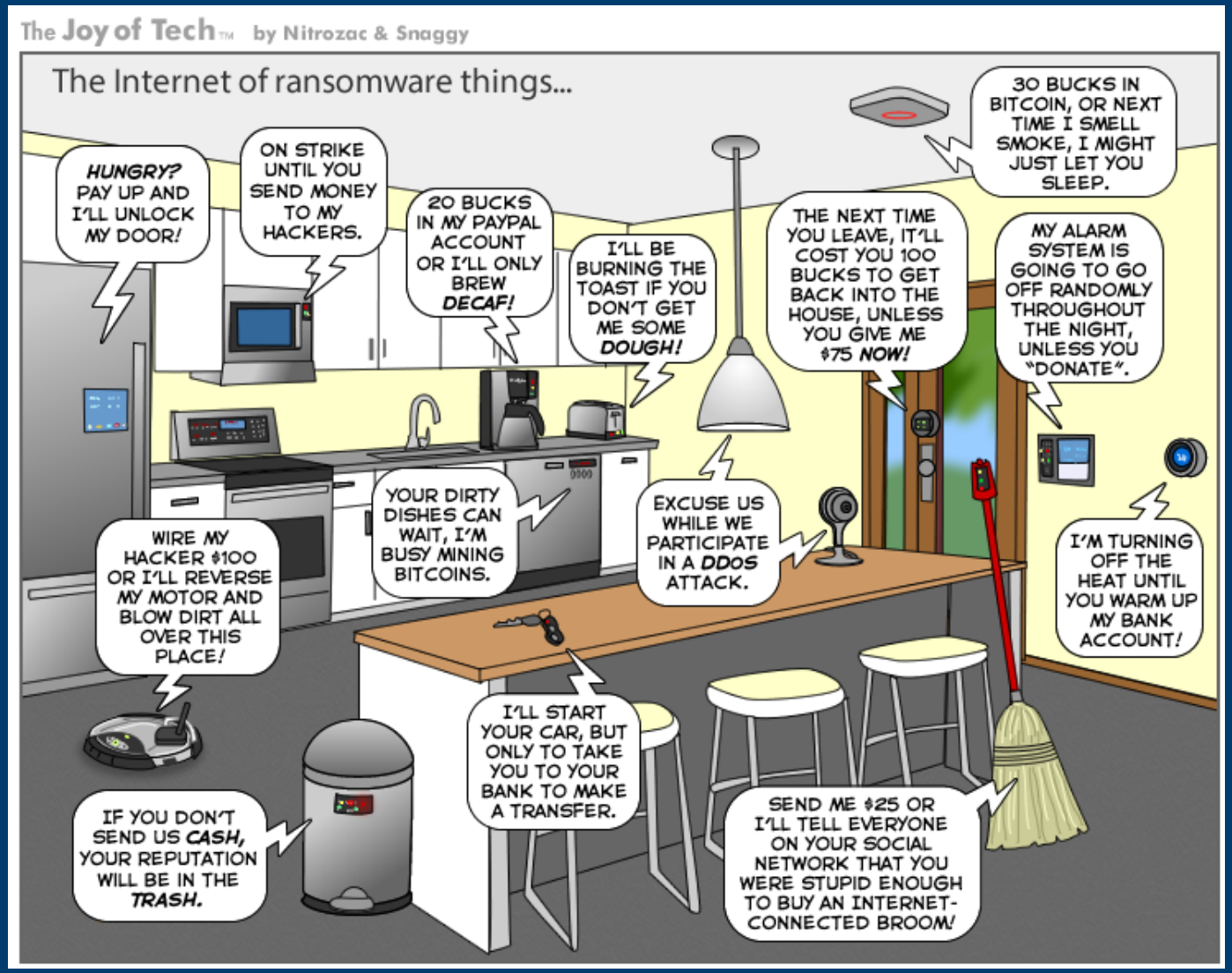
What if all the devices in your life could connect to the internet?

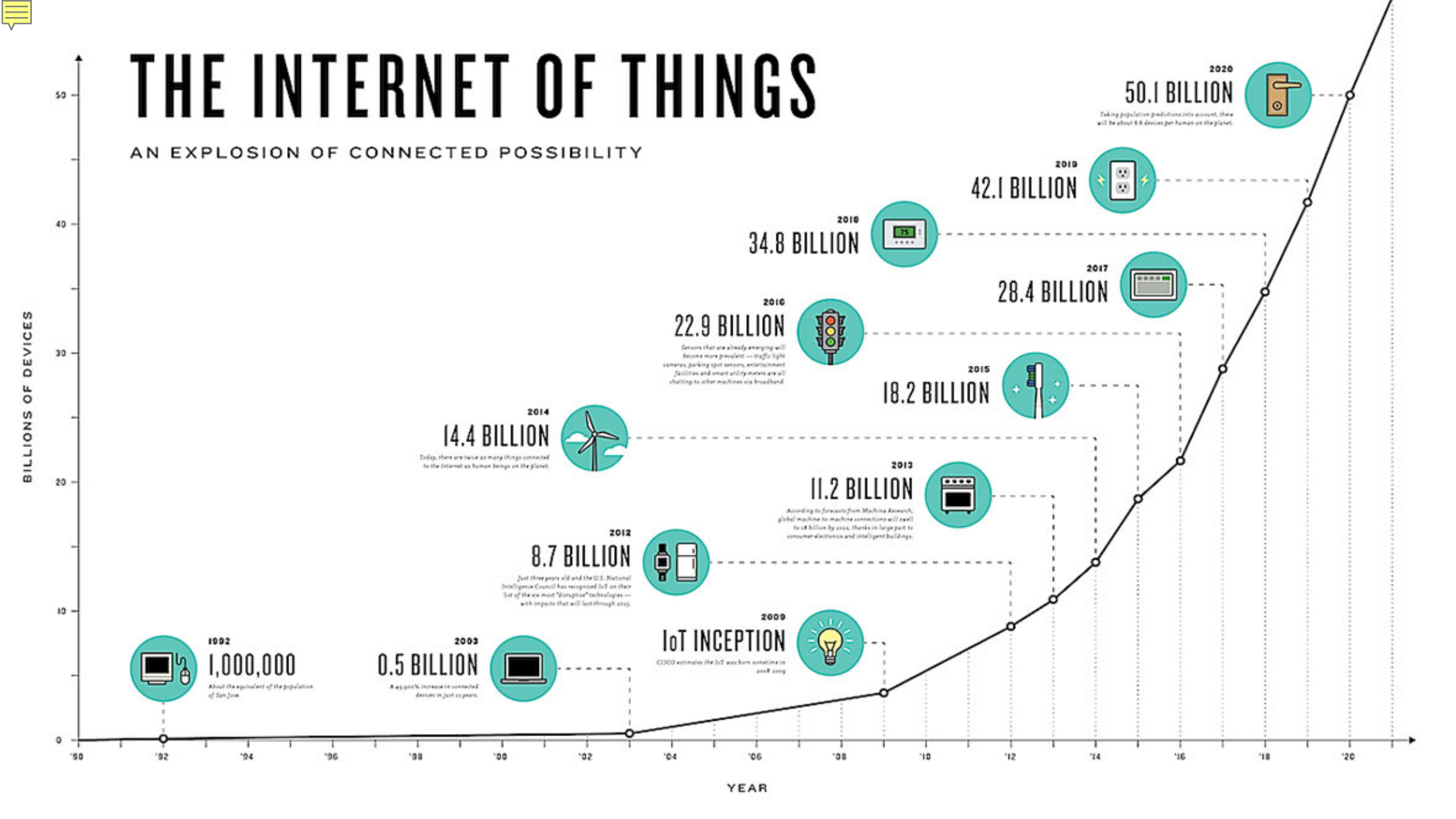
Everything: computers, smart phones, clocks, speakers, lights, doorbells, cameras, windows, window blinds, hot water heaters, appliances, cooking utensils – you name it.

What if those devices could all communicate, send information and take commands?



Internet of things



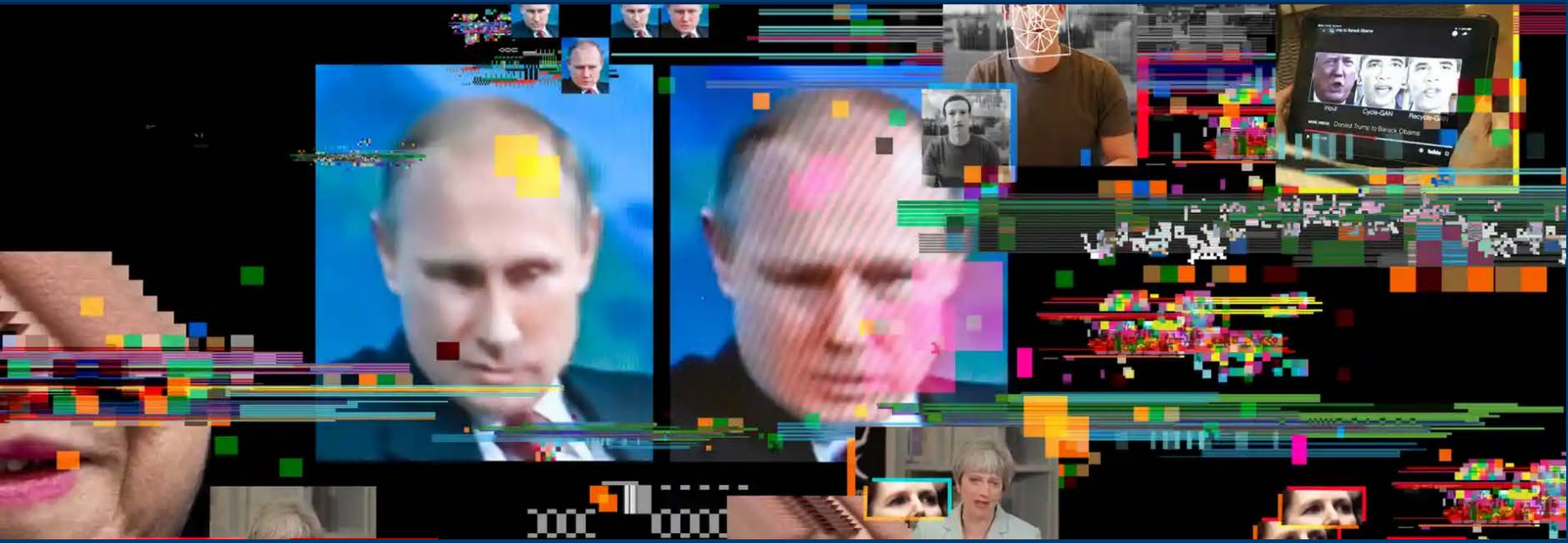

THE INTERNET OF THINGS
AN EXPLOSION OF CONNECTED POSSIBILITY
BILLIONS OF DEVICES
50
40
30
20
10
0
'90
'92
'94
'96
'98
'00
'02
'04
'06
'08
'10
'12
'14
'16
'18
'20
YEAR
1992
1,000,000
About the equivalent of the population of San Jose.
2003
0.5 BILLION
A 49,900% increase in connected devices in just 10 years.
2009
IoT INCEPTION
CISCO estimates the IoT was born sometime in 2008 2009.
2012
8.7 BILLION
Just three years old and the U.S. National Intelligence Council has recognized IoT on their list of the six most "disruptive" technologies — with impacts that will last through 2025.
2014
14.4 BILLION
Today, there are twice as many things connected to the Internet as human beings on the planet.
2016
22.9 BILLION
Sensors that are already emerging will become more prevalent — traffic light cameras, parking spot sensors, entertainment facilities and smart utility meters are all chatting to other machines via broadband.
2018
34.8 BILLION
2019
42.1 BILLION
2020
50.1 BILLION
Taking population predictions into account, there will be about 6.6 devices per human on the planet.
2013
11.2 BILLION
According to forecasts from Machina Research, global machine-to-machine connections will swell to 18 billion by 2022, thanks in large part to consumer electronics and intelligent buildings.
2015
18.2 BILLION
2017
28.4 BILLION

Internet of things - Stuxnet

How does it work:

- Malware enters via a USB and is shielded by a certificate that looks authentic
- It then looks for specific software that handles the nuclear centrifuge
- Once it finds a target, it downloads the most recent version of itself and begins compromising the organization's zero day vulnerabilities
- Specifically, it begins spinning the centrifuges to failure – all the while telling the controllers everything is fine – until it's too late.

Deepfakes and the rise of AI



Deepfakes and the rise of AI

#Channel4 #All4 #Deepfake

Deepfake Queen: 2020 Alternative Christmas Message

2,353,445 views • Dec 25, 2020 25K 5.6K SHARE SAVE

This Game of Thrones Deepfake Made Jon Snow Apologize for Season 8 (Nerdist News Edition)

Deepfakes and the rise of AI

So, what's the problem:

- Dancing Queen, Jon Snow and Tom Cruise = innovative and funny
- 96 percent are pornographic in nature – mapping female celebs, politicians, etc. onto existing pornographic videos
- Fake videos are spreading beyond the celebrity world to fuel revenge porn
- Deepfake technology is being weaponized against women

Deepfakes and the rise of AI

We can figure that out, so what else?

- Deepfake technology can create convincing but entirely fictional photos from scratch
  - Non-existent Bloomberg journalist, “Maisy Kinsley”, who had a profile on LinkedIn and Twitter, was probably a deepfake.
  - “Katie Jones”, claimed to work at the Center for Strategic and International Studies, but is thought to have been created on LinkedIn for spying
- Audio can be deepfaked too, to create “voice skins” or ”voice clones” of public figures

This is a little scary. What can we do?

- Phishing may be *one of the oldest tricks in the book*…
- Know the red flags
- Verify the source
- Misery loves company (vishing, smishing, etc.)
- If it feels phishy… it probably is

This is a little scary. What can we do?

- Install antivirus protection on your personal devices
- Use encryption and VPN especially on public wifi
- Listen to your email security tools
- Educate those around your circle of influence
- Use passphrases instead of passwords
- Download files only from sources you can trust
- Be careful of too good to be true social media ads

This is a little scary. What can we do?

- Monitor your devices – all of them
- Change your Wi-Fi password often
- Turn off your Wi-Fi when you're not using it
- Hide by using a Virtual Private Network or VPN
- Research devices – specifically surrounding security
- Know who has access to what wireless-wise

This is a little scary. What can we do?

- Is the message controversial or polarizing?
- Use several trusted sources to confirm the video's message
- Take off your passion hat and put on your thinking cap
- Unrealistic hair
- Strange eyes
- Can you see individual teeth?
- Does the face and body sync up?

UMB

CYBERSECURITY IS EVERYONE'S JOB.

INCLUDING YOURS.

CYBERSECURITY AWARENESS MONTH

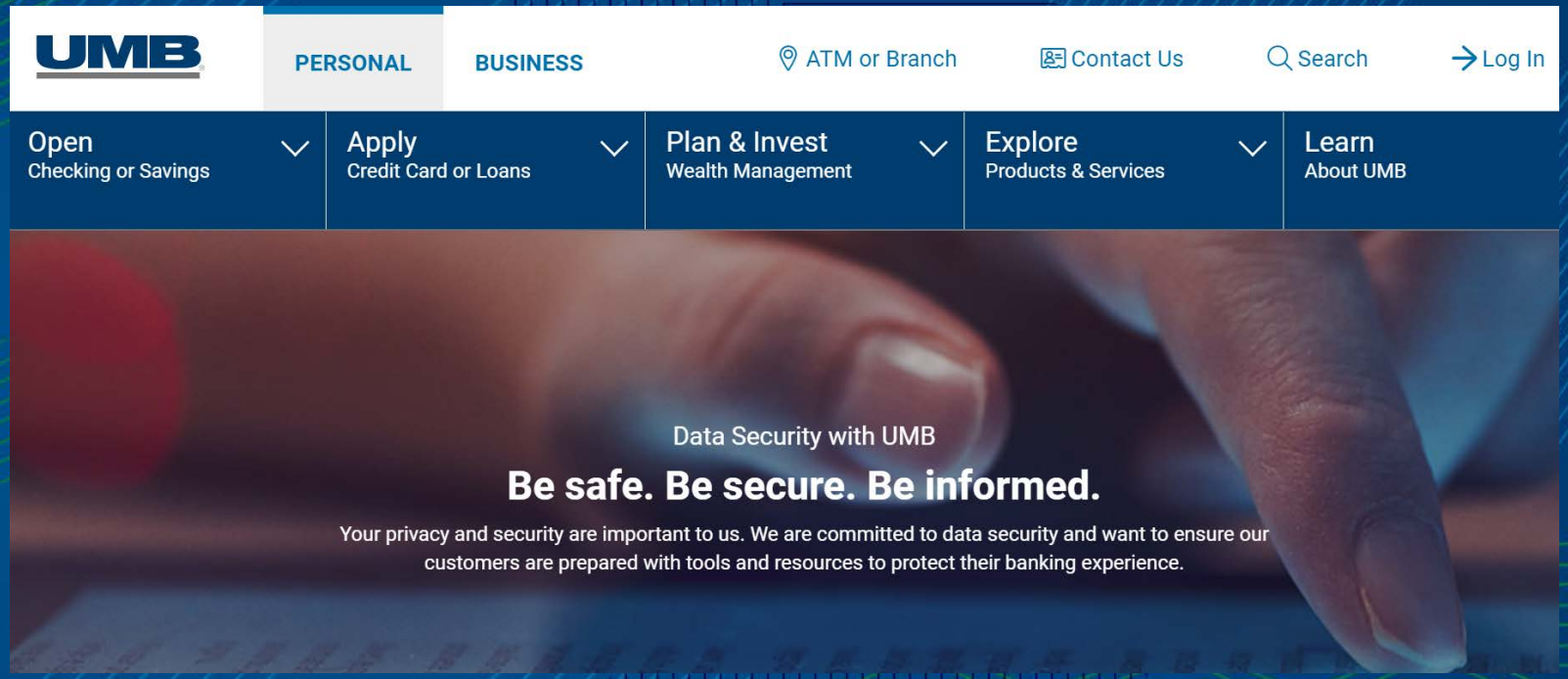
STAYSAFEONLINE.ORG/
CYBERSECURITY-AWARENESS-MONTH

UMB

Think of your personal information like your toothbrush. *Don't share it.*

A message from the
UMB Security Awareness Team
umb.com/security

Thank you.



UMB.com/Security

UMB.com/Blog (Keywords information security)