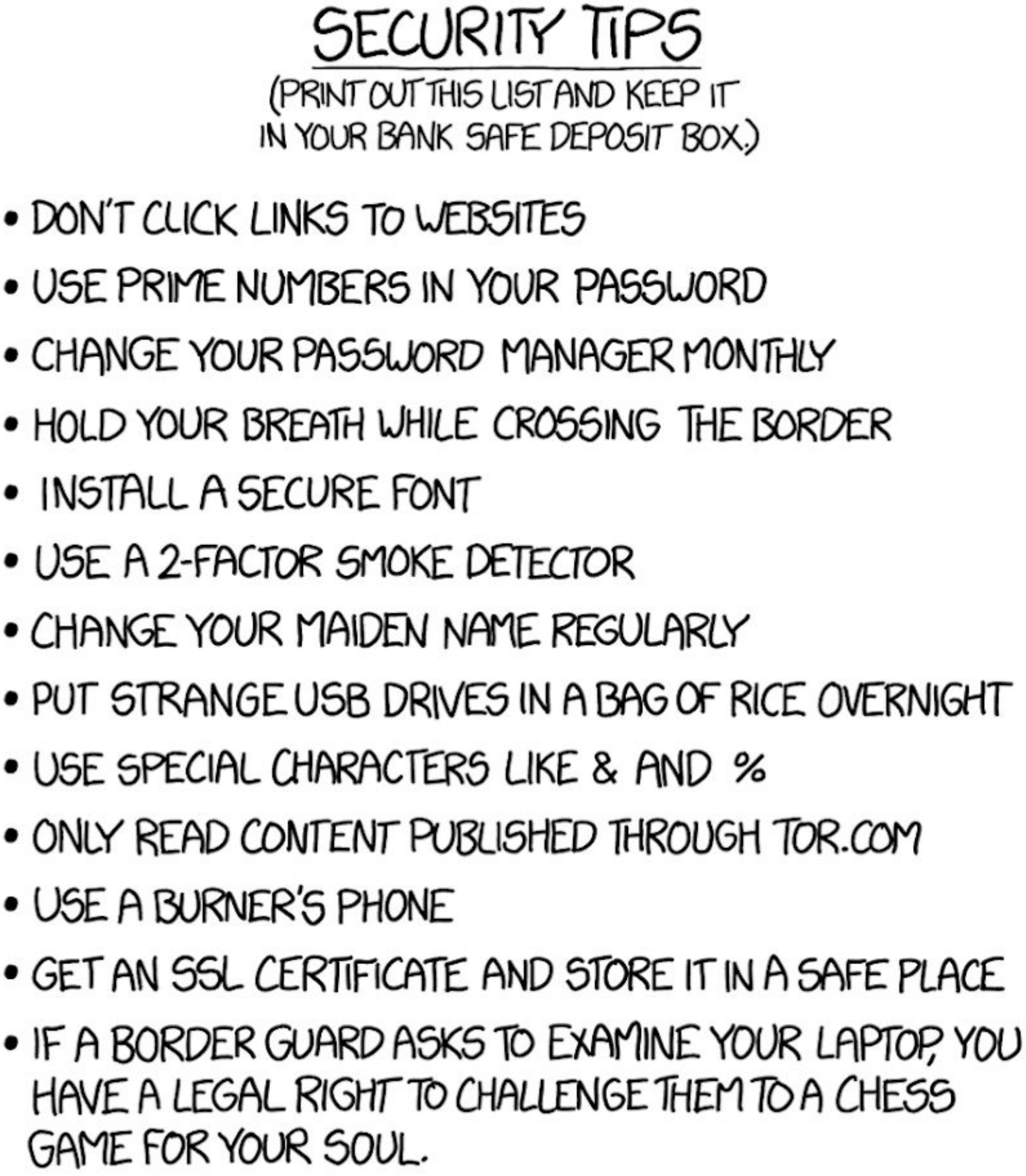
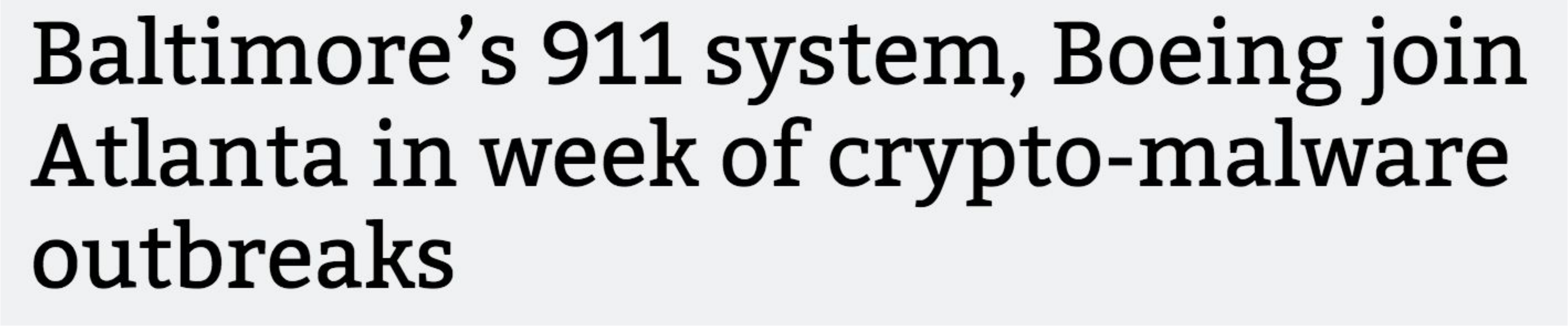


SECURITY TIPS

(PRINT OUT THIS LIST AND KEEP IT
IN YOUR BANK SAFE DEPOSIT BOX.)

- DON'T CLICK LINKS TO WEBSITES
- USE PRIME NUMBERS IN YOUR PASSWORD
- CHANGE YOUR PASSWORD MANAGER MONTHLY
- HOLD YOUR BREATH WHILE CROSSING THE BORDER
- INSTALL A SECURE FONT
- USE A 2-FACTOR SMOKE DETECTOR
- CHANGE YOUR MAIDEN NAME REGULARLY
- PUT STRANGE USB DRIVES IN A BAG OF RICE OVERNIGHT
- USE SPECIAL CHARACTERS LIKE & AND %
- ONLY READ CONTENT PUBLISHED THROUGH TOR.COM
- USE A BURNER'S PHONE
- GET AN SSL CERTIFICATE AND STORE IT IN A SAFE PLACE
- IF A BORDER GUARD ASKS TO EXAMINE YOUR LAPTOP, YOU HAVE A LEGAL RIGHT TO CHALLENGE THEM TO A CHESS GAME FOR YOUR SOUL.

Recently…



Baltimore’s 911 system, Boeing join Atlanta in week of crypto-malware outbreaks

Under Armour Data Breach Compromises 150 Million User Accounts

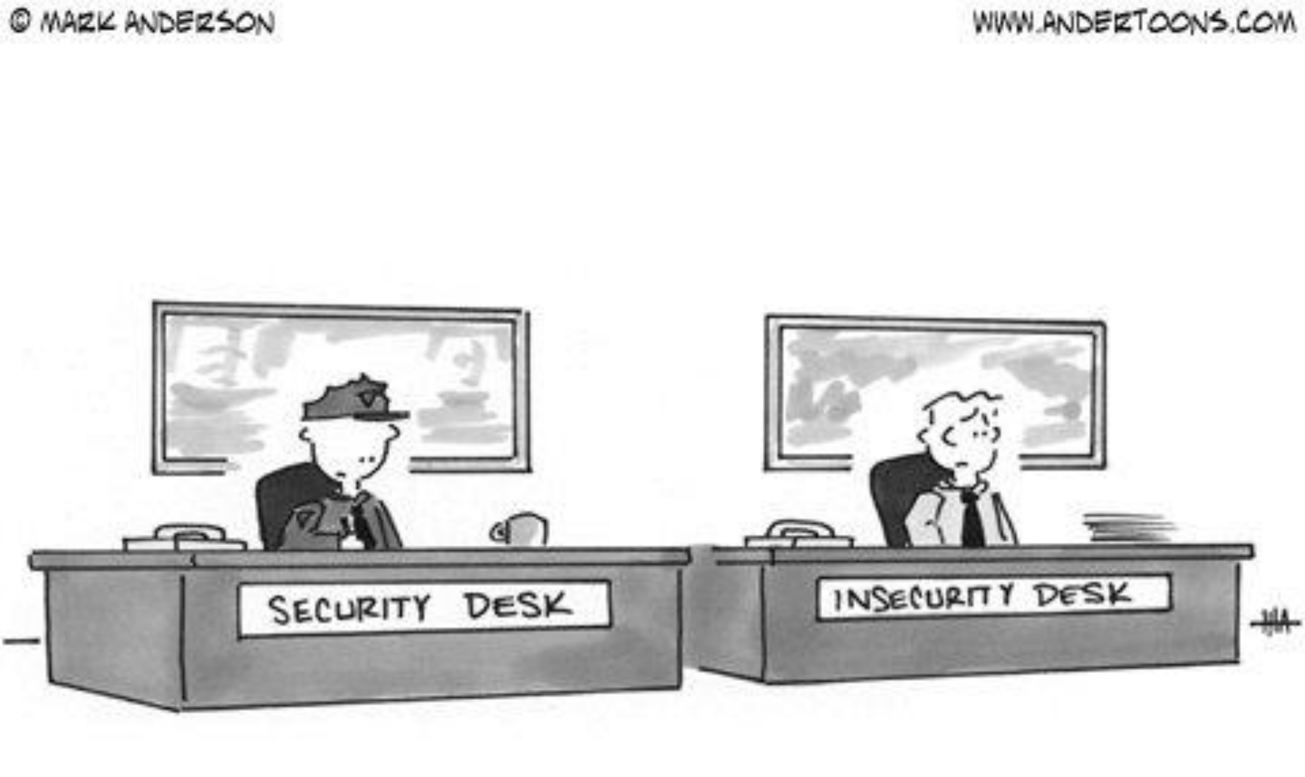
02 APR 18

Panerabread.com Leaks Millions of Customer Records

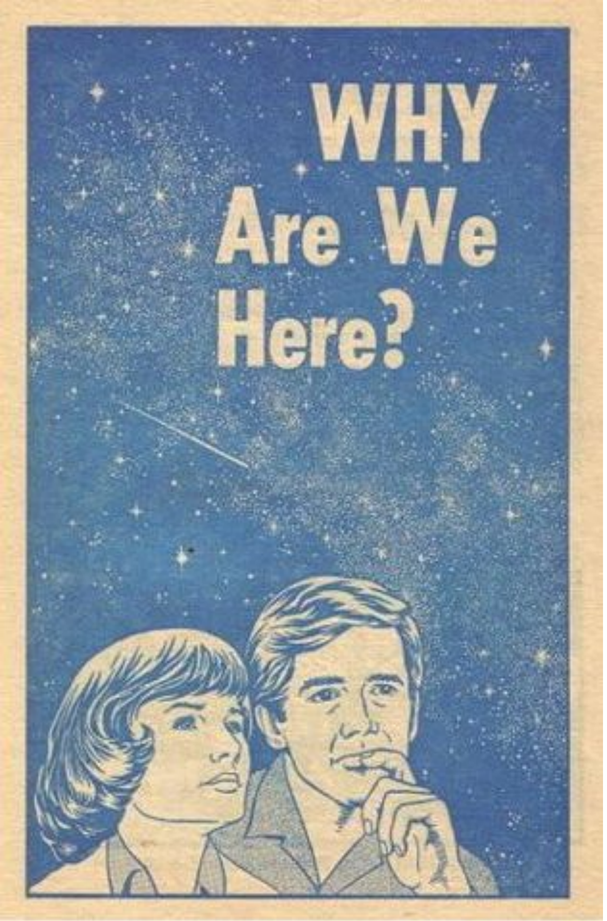
Cybersecurity Awareness Training

RoundTable TECHNOLOGY

Icebreaker



At which desk do you feel like you belong?



CyberSecurity can seem overwhelming, complex and sometimes even scary.

But much of cybersecurity is manageable by non-technical people and most cybersecurity depends on people and behavior.

It turns out there are some pretty basic things you can do to make yourself and your organization significantly more secure.

Today, we'll talk about those things.

Things you can do that make a big difference

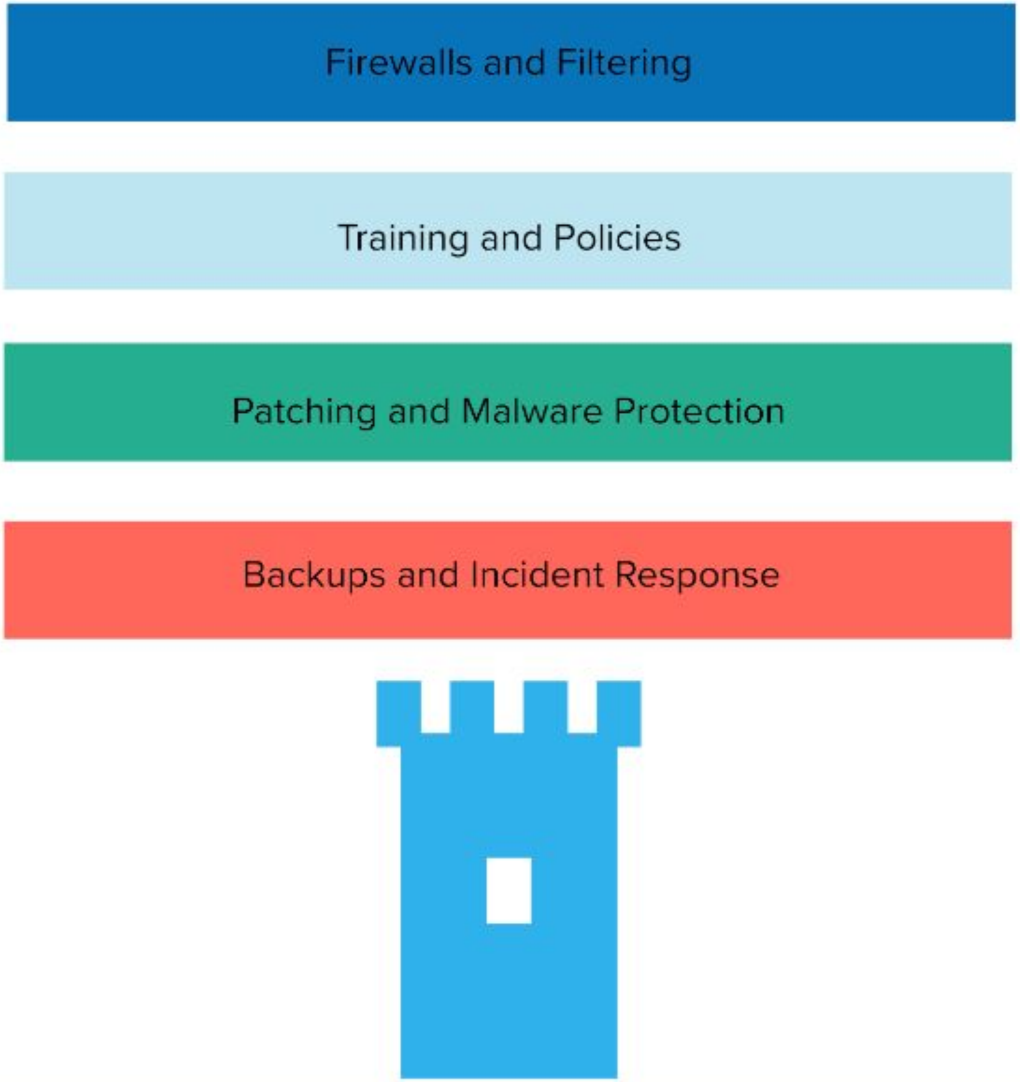
• Nurture	A security culture at your organization
• Educate	Yourself and others about tactics used to steal your info
• Protect	Your accounts and devices with secure practices
• Verify	When in (ANY) doubt, VERIFY!

NOT something you should do. →

"Then the messenger shouldn't have been such a jerk."

Layers of Defense

Malicious actors, malware, randsomware,
failing hard drives, stolen laptops,
lost smartphones, phishing & errors



Firewalls and Filtering

Training and Policies

Patching and Malware Protection

Backups and Incident Response

A Challenge: Can you stay awake for…

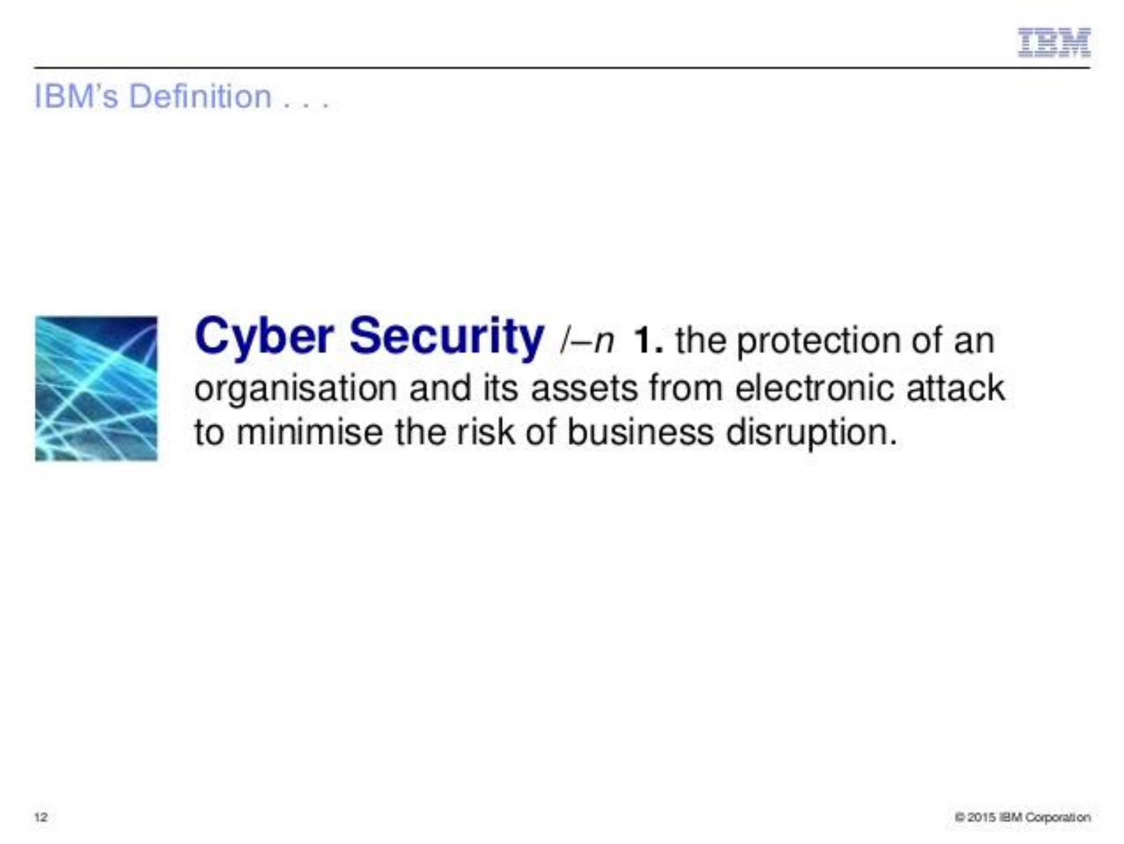
Three Slides of Boring Stuff

We want to explain cybersecurity because it's a term we all see a lot.

It might be a little boring, but it's only three slides and we'll go fast

Key Term

Cybersecurity



IBM's Definition . . .

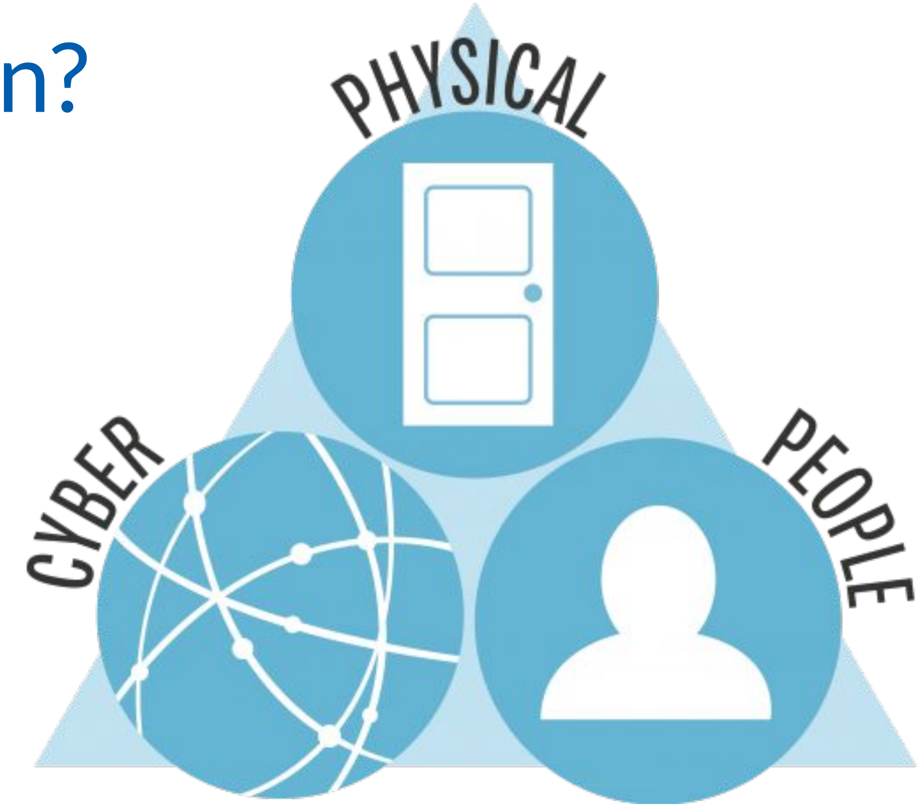
Cyber Security */–n* **1.** the protection of an organisation and its assets from electronic attack to minimise the risk of business disruption.

12

Security Triad

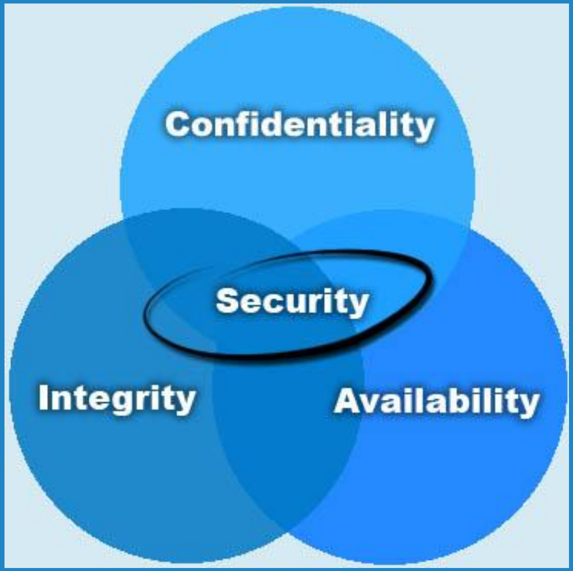
Where do people fit in?

Everywhere



The CIA Security Triad

(yes another triad)



C - How bad would it be if the information was exposed

I - How bad would it be if the information was lost

A - How bad would it be if the information was not available

You made it through three slides of boring stuff
Congratulations!

Key Term

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Vishing (Voice Phishing) and Spear Phishing (targeted phishing) are other types of phishing)

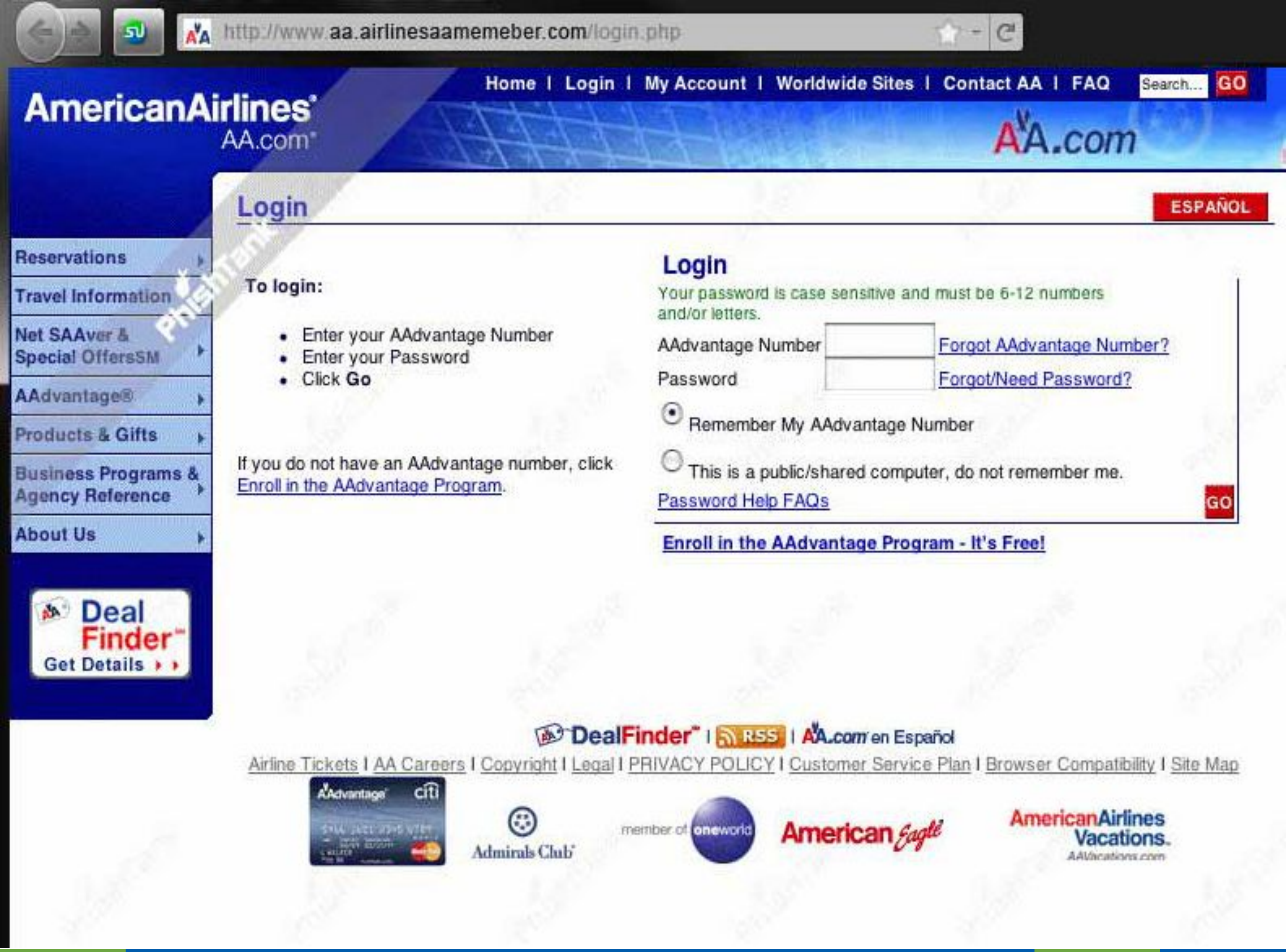
Phishing

Phish or not a Phish?

Phish or not a Phish?

Take a look at the website we will display next. We'll leave it up for 10 seconds, then ask everyone if they think it is a phish (fake website) or not a phish (legitimate).

P.S. You will notice a watermark "Phishtank" on most of the images.
This is NOT a signifier of phish or not a phish status.



http://www.aa.airlinesaamemeber.com/login.php
Home | Login | My Account | Worldwide Sites | Contact AA | FAQ
Search...
GO
AmericanAirlines
AA.com
AA.com
ESPAÑOL
Reservations
Travel Information
Net SAAver & Special OffersSM
AAdvantage®
Products & Gifts
Business Programs & Agency Reference
About Us
Deal Finder
Get Details
GO
DealFinder | RSS | AA.com en Español
Airline Tickets | AA Careers | Copyright | Legal | PRIVACY POLICY | Customer Service Plan | Browser Compatibility | Site Map
AAdvantage citi
Admirals Club
member of oneworld
American Eagle
AmericanAirlines Vacations
AAVacations.com

Login

To login:

- Enter your AAdvantage Number
- Enter your Password
- Click **Go**

If you do not have an AAdvantage number, click Enroll in the AAdvantage Program.

Login

Your password is case sensitive and must be 6-12 numbers and/or letters.

AAdvantage Number ____ Forgot AAdvantage Number?

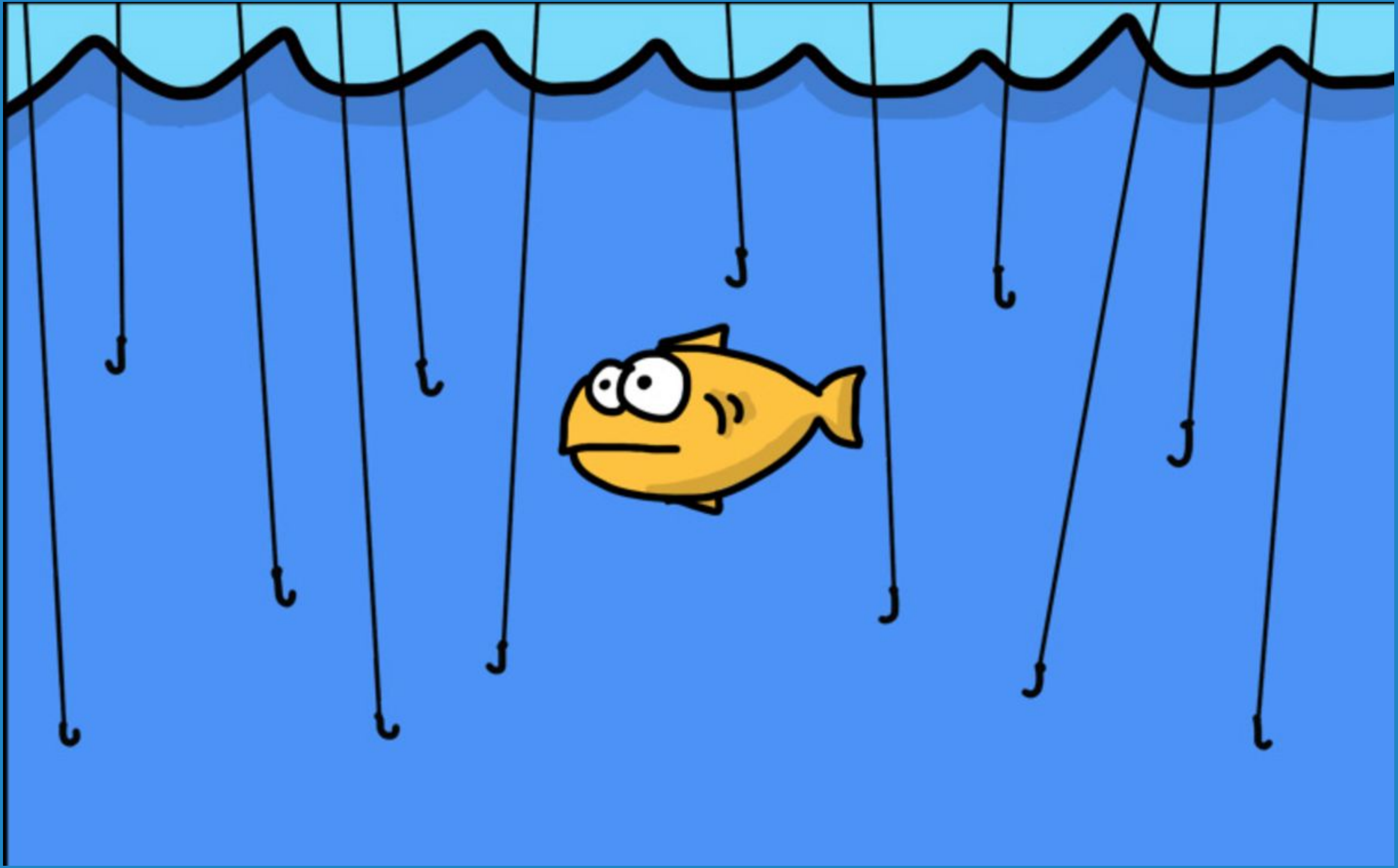
Password ____ Forgot/Need Password?

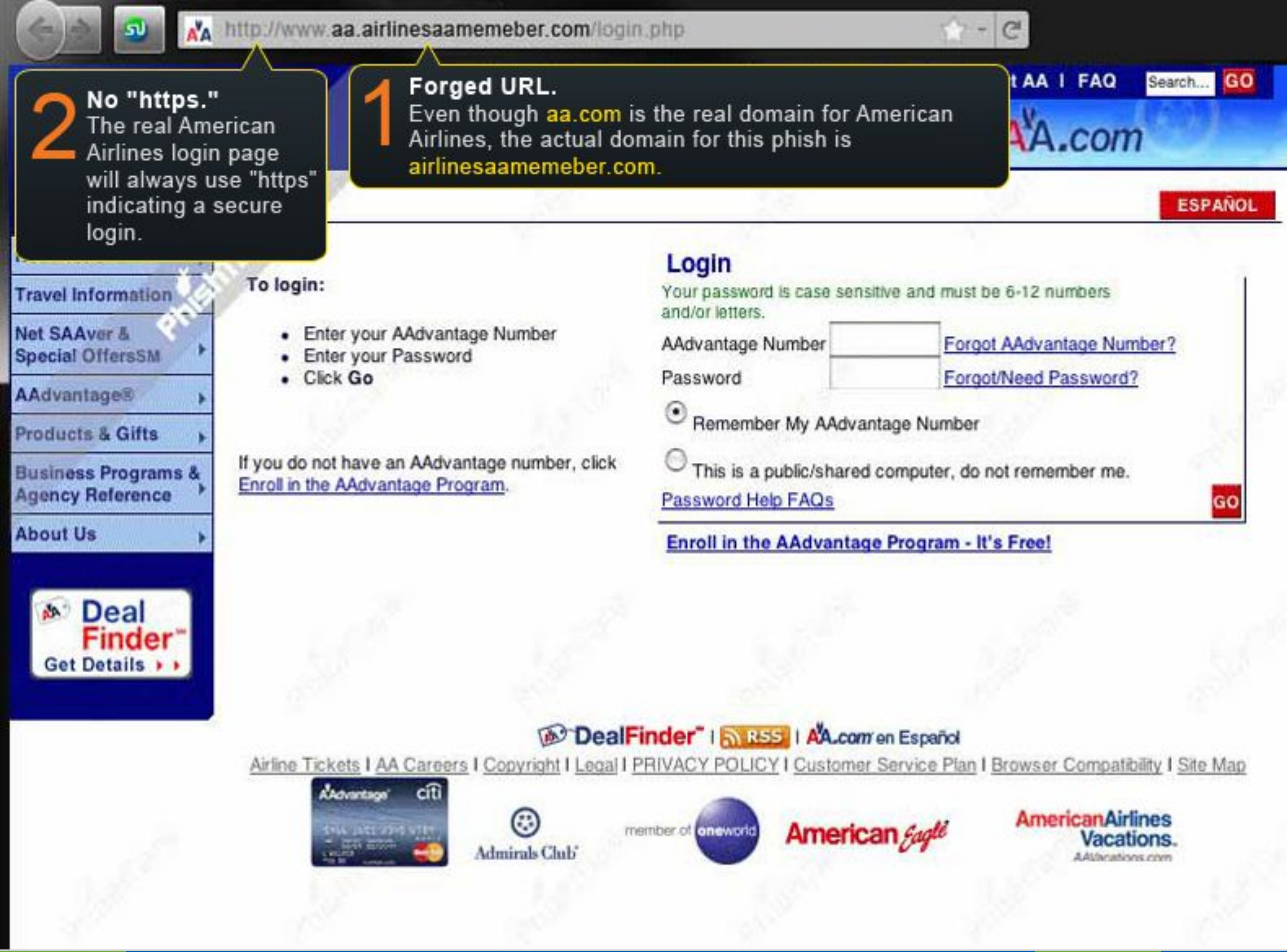
● Remember My AAdvantage Number

○ This is a public/shared computer, do not remember me.

Password Help FAQs

Enroll in the AAdvantage Program - It's Free!





1 **Forged URL.** Even though aa.com is the real domain for American Airlines, the actual domain for this phish is airlinesaamemeber.com.

2 **No "https."** The real American Airlines login page will always use "https" indicating a secure login.

http://www.aa.airlinesaamemeber.com/login.php

Login

Your password is case sensitive and must be 6-12 numbers and/or letters.

AAdvantage Number [ ] Forgot AAdvantage Number?

Password [ ] Forgot/Need Password?

● Remember My AAdvantage Number

○ This is a public/shared computer, do not remember me.

Password Help FAQs

GO

Enroll in the AAdvantage Program - It's Free!

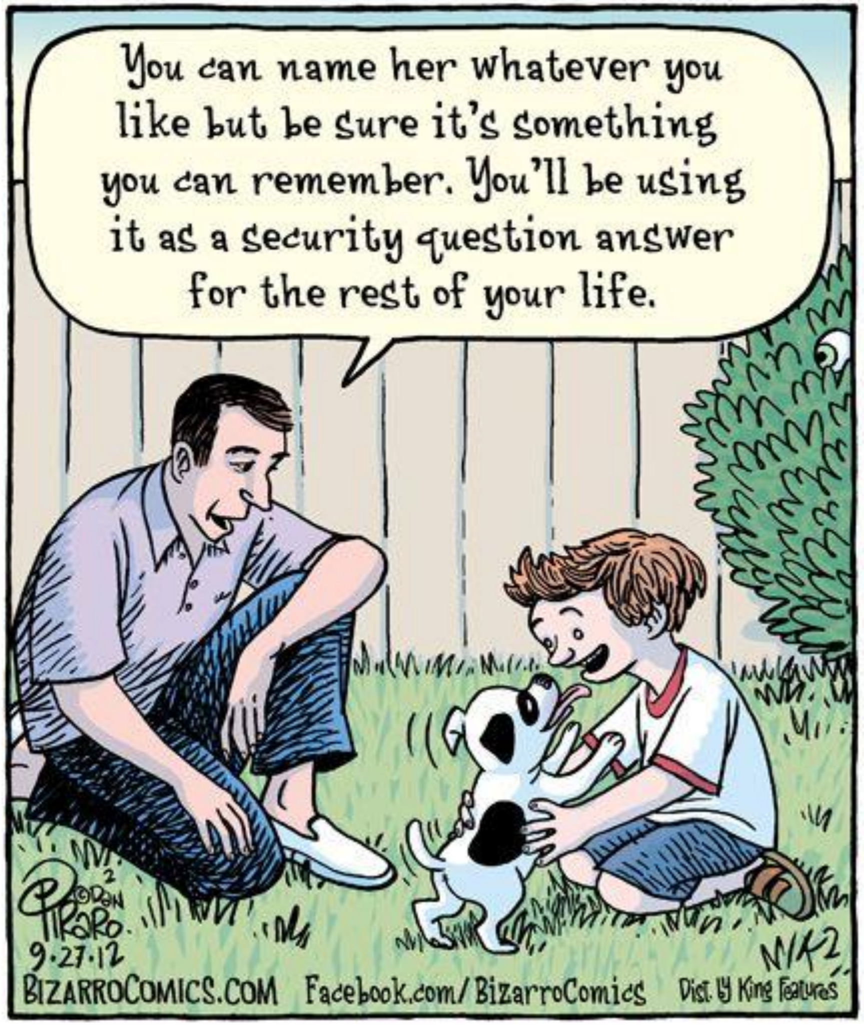
To login:

- Enter your AAdvantage Number
- Enter your Password
- Click **Go**

If you do not have an AAdvantage number, click Enroll in the AAdvantage Program.

t AA I FAQ
Search...
GO
AA.com
ESPAÑOL
Travel Information
Net SAAver & Special OffersSM
AAdvantage®
Products & Gifts
Business Programs & Agency Reference
About Us
Deal Finder™
Get Details
DealFinder™ | RSS | AA.com en Español
Airline Tickets | AA Careers | Copyright | Legal | PRIVACY POLICY | Customer Service Plan | Browser Compatibility | Site Map
AAdvantage citi
Admirals Club
member of oneworld
American Eagle
AmericanAirlines Vacations.
AAVacations.com

Can I have your personal information?


You can name her whatever you like but be sure it's something you can remember. You'll be using it as a security question answer for the rest of your life.
©Dan Piraro 9·27·12
BIZARROCOMICS.COM
Facebook.com/BizarroComics
Dist. by King Features

What's YOUR My Little Pony name?

Phishing for Passwords

Threat Modeling

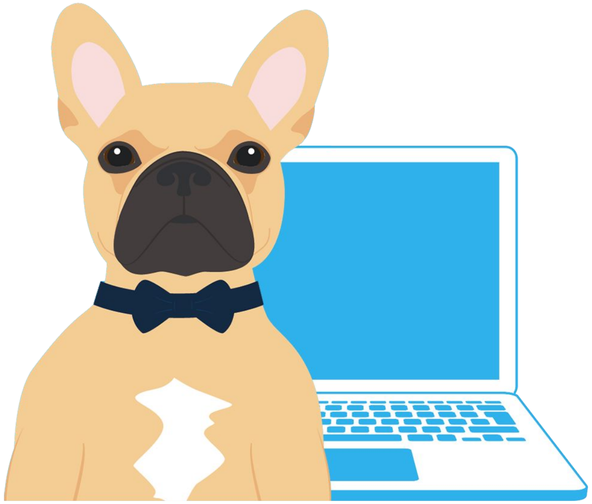
The core questions to ask:
(from the Electronic Frontier Foundation)

HAND OVER THE MONEY, OR I'LL EXPLAIN THE ABSURDITY OF ALL HUMAN ACTIVITY
©2016 Stivers
Thanks to Dave Bass
EXISTENTIAL THREAT

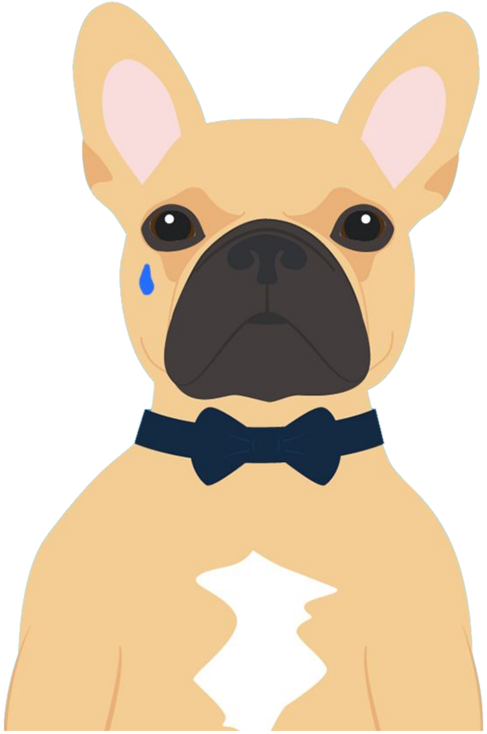
- What do you want to protect?
- Who do you want to protect it from?
- How likely is it that you will need to protect it?
- How bad are the consequences if you fail?
- How much effort are you willing to expend?

The Threat Model we ALL have in common

Risk is part of Existence

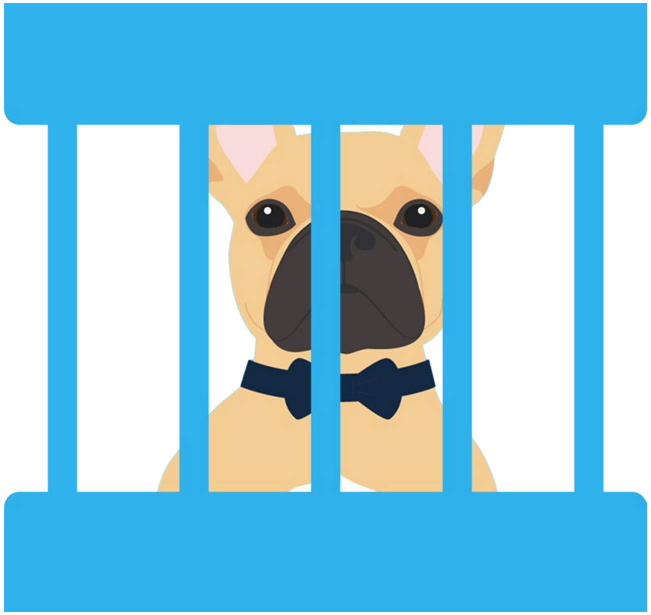


Avoid

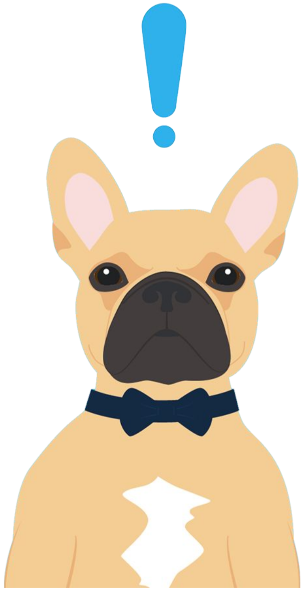


Reduce

Transfer



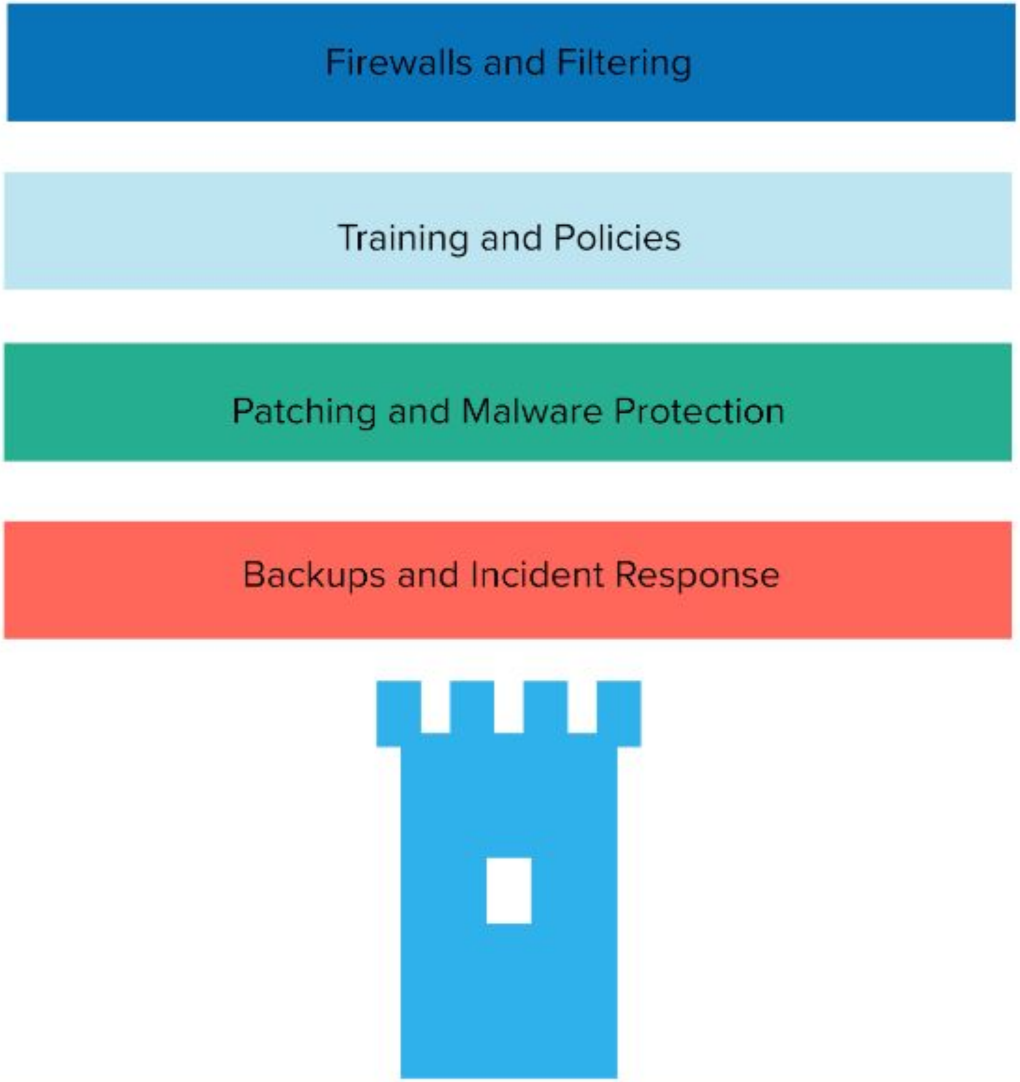
Accept



Ways we get breached

Layers of Defense

Malicious actors, malware, randsomware,
failing hard drives, stolen laptops,
lost smartphones, phishing & errors



Firewalls and Filtering

Training and Policies

Patching and Malware Protection

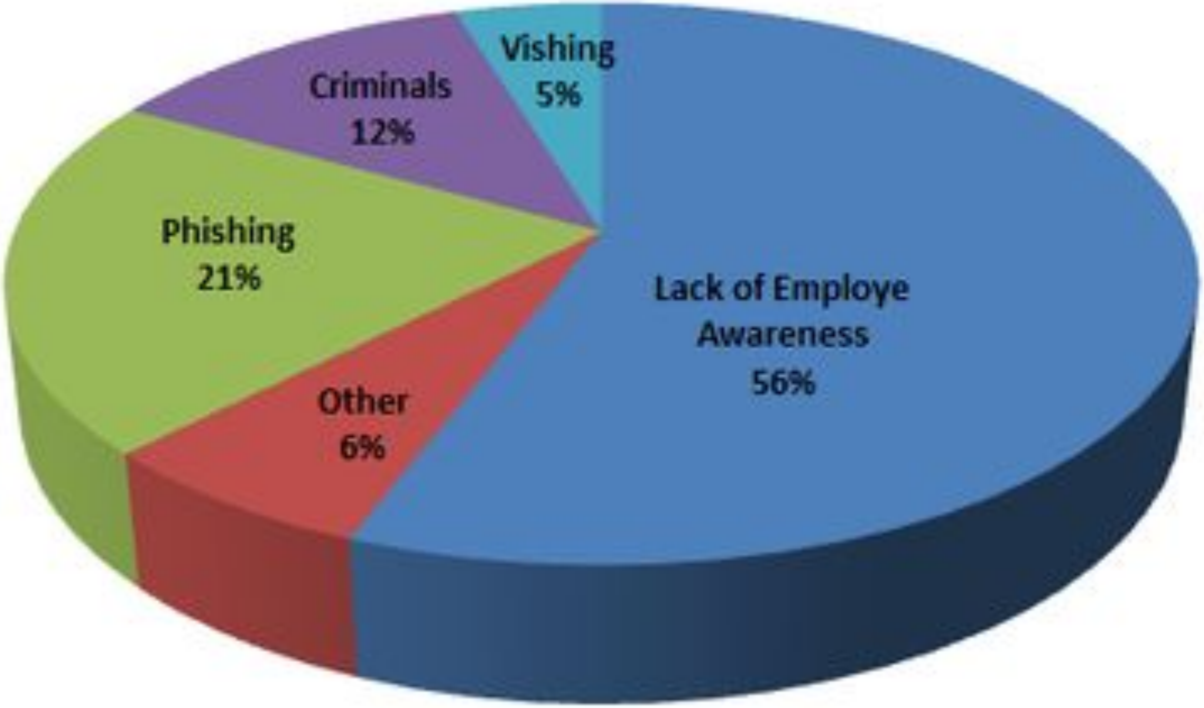
Backups and Incident Response

Social Engineering

Key Term

The manipulation of our human instinct to help

What's the most dangerous social engineering threat to organizations?



Characteristics

- Initiation
- Urgency
- Fear
- Authority

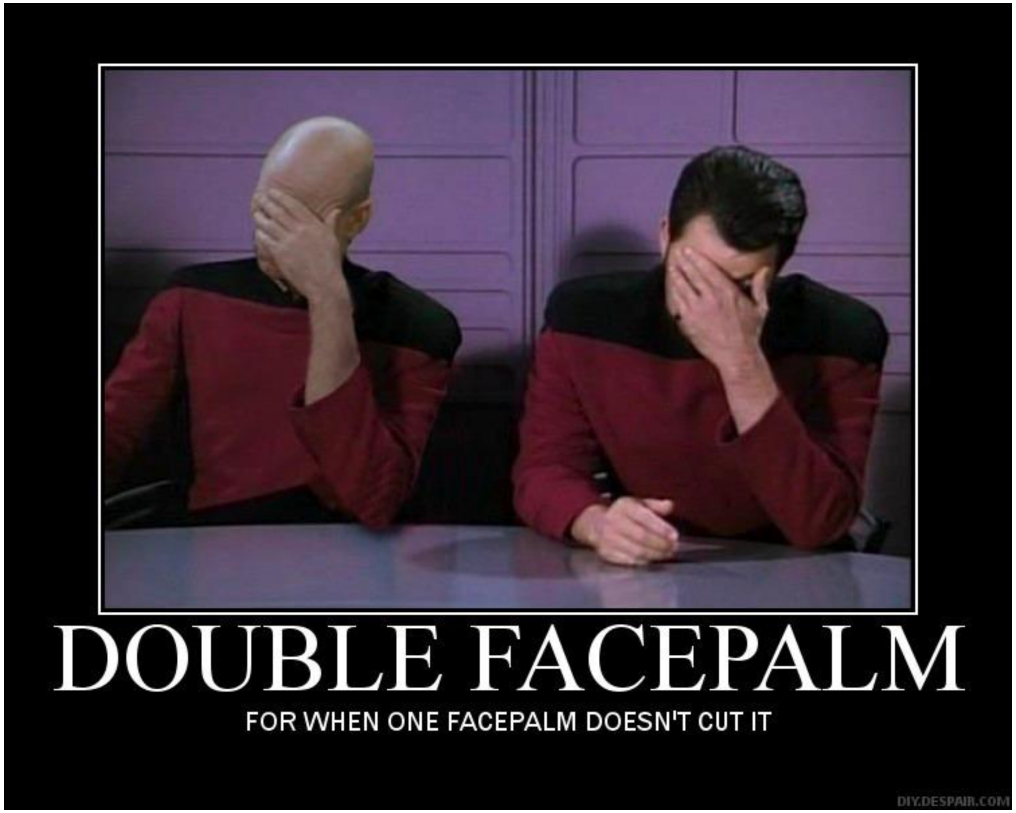
Asking for

- Clicks
- Money
- Credentials
- Information

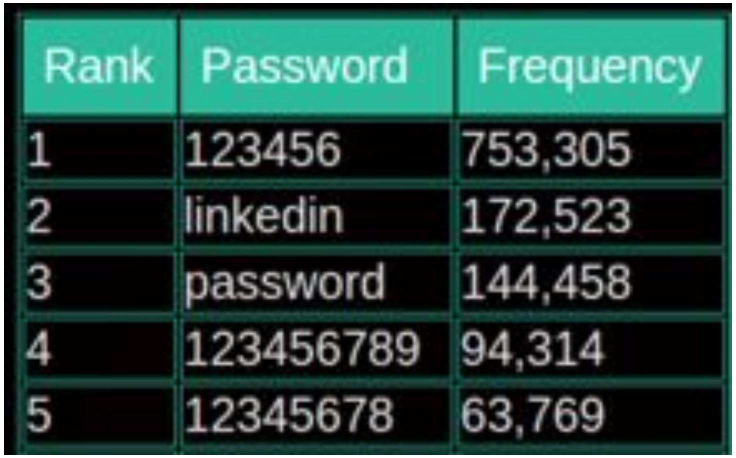
Book recommendation - Gift of Fear by Gavin DeBecker

You would have to send me a secure pin through a text message?

123456 is THE BEST password

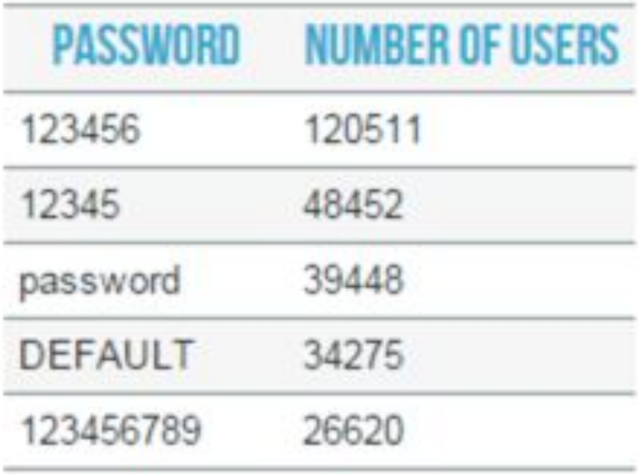


LinkedIn breach (2012)



Rank	Password	Frequency
1	123456	753,305
2	linkedin	172,523
3	password	144,458
4	123456789	94,314
5	12345678	63,769

Ashley Madison breach (2015)



PASSWORD	NUMBER OF USERS
123456	120511
12345	48452
password	39448
DEFAULT	34275
123456789	26620

What makes the strongest passwords?

7!G2Kq@q

Or

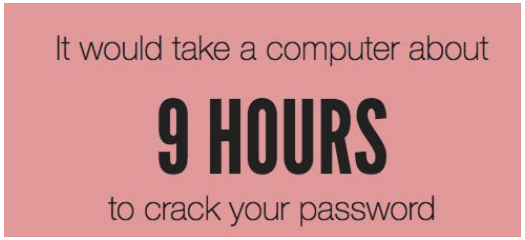
xCuBZE$$%^s2

Or

I like to eat donuts on Wednesdays.

Question: Which of these is the strongest password?

7!G2Kq@q

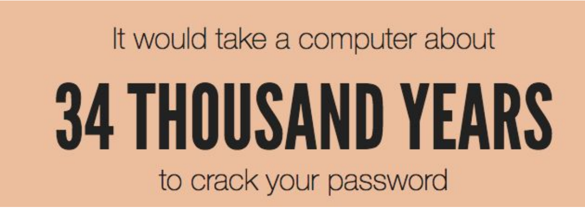


It would take a computer about

9 HOURS

to crack your password

xCuBZE$$%^s2

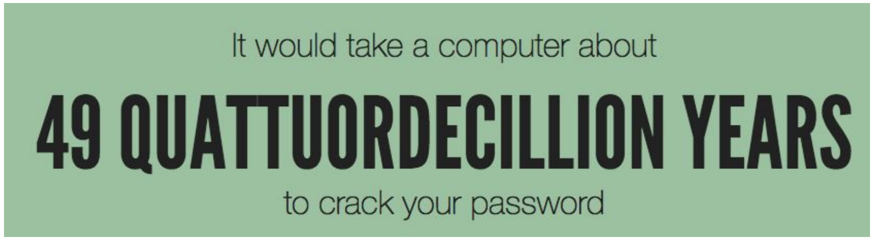


It would take a computer about

34 THOUSAND YEARS

to crack your password

I like to eat donuts on Wednesdays.



It would take a computer about

49 QUATTUORDECILLION YEARS

to crack your password

Scores from: https://howsecureismypassword.net/

Human brains are not good at making and remembering long, complex and random alphanumeric strings.

WHAT DOES MY FOREHEAD SAY?
I KEEP FORGETTING MY PASSWORD, SO I WROTE IT ON MY HEAD.
IS YOUR PASS–WORD 123?
I JUST SAID I DON'T KNOW.
www.dilbert.com scottadams@aol.com
6-11-07 © 2007 Scott Adams, Inc./Dist. by UFS, Inc.

And wait, it gets worse...

Even Complex Passwords aren't great

- They can still get phished
- They can still be reused in multiple places
- They can still be shared in insecure ways (e.g. plain text)
- They can still be part of a larger breach
- They can still be captured by keystroke loggers

Password Managers to the Rescue

Top Password Managers

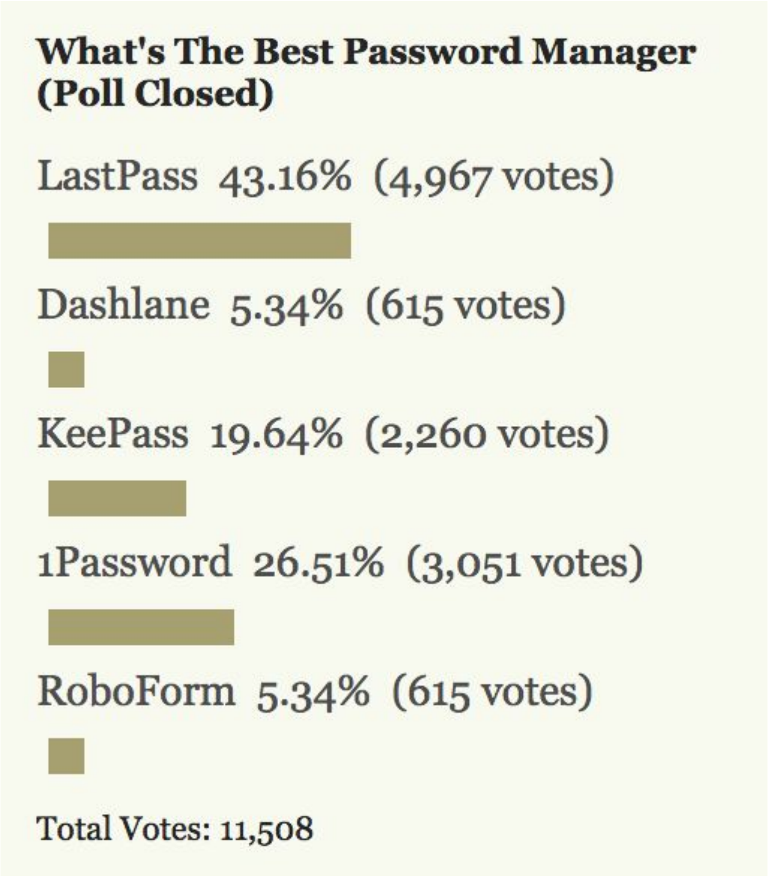
LastPass

1Password

KeePass

dashlane

RoboForm



What's The Best Password Manager (Poll Closed)

LastPass 43.16% (4,967 votes)

Dashlane 5.34% (615 votes)

KeePass 19.64% (2,260 votes)

1Password 26.51% (3,051 votes)

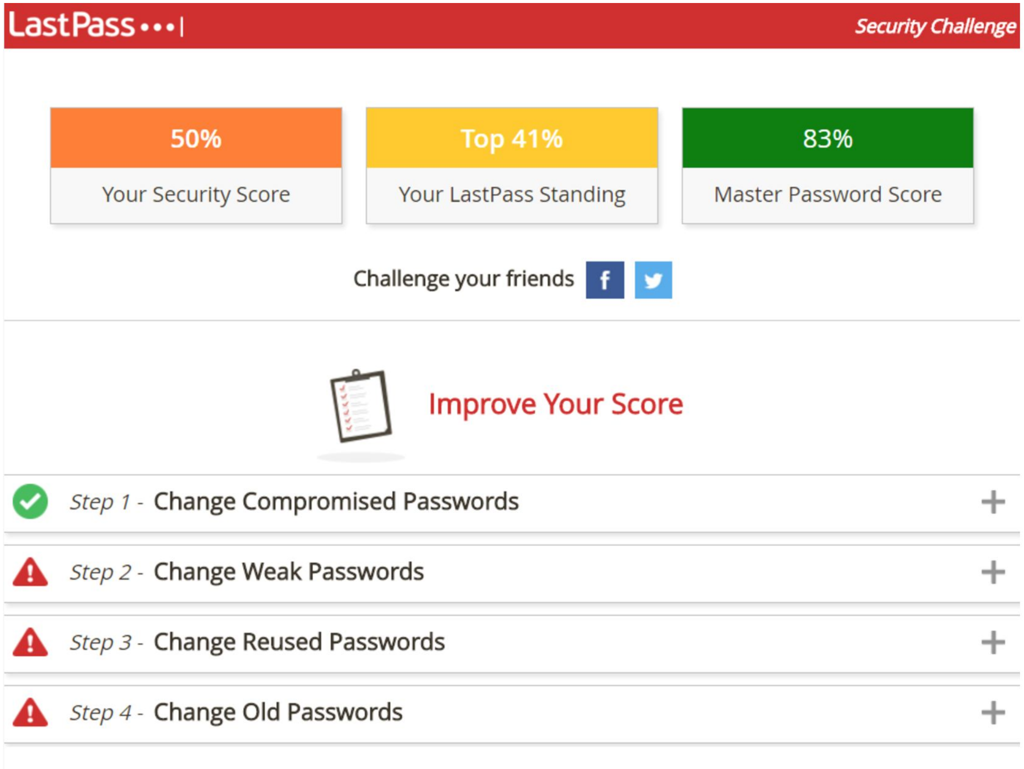
RoboForm 5.34% (615 votes)

Total Votes: 11,508

Source: Lifehacker January 2015

Password Managers - Basics

- Create long, complex and random passwords.
  - It's literally their job.
- Inexpensive (generally <$30/year/person)
- Protects against phishing attacks
- Can audit all your passwords



LastPass•••| Security Challenge

50%	Top 41%	83%
Your Security Score	Your LastPass Standing	Master Password Score

Challenge your friends f

Improve Your Score

✓ *Step 1 -* Change Compromised Passwords +

⚠ *Step 2 -* Change Weak Passwords +

⚠ *Step 3 -* Change Reused Passwords +

⚠ *Step 4 -* Change Old Passwords +

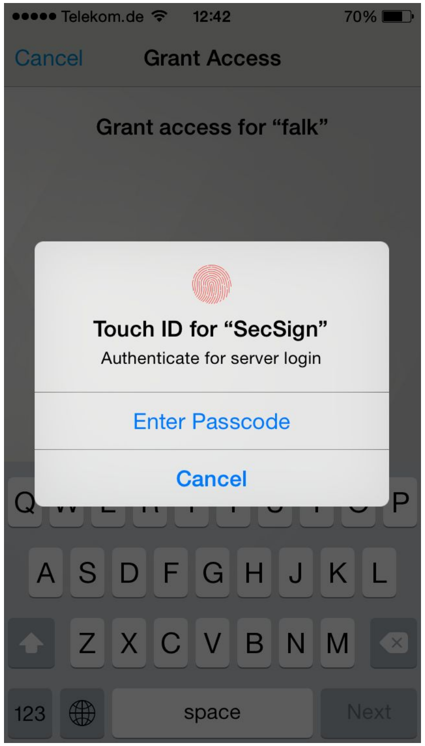
Ways to Authenticate

1. Something you know (username, password)
2. Something you have (smartphone, usb key)
3. Something you are (fingerprint, voice recognition)

A form of 2FA we all use already

Common Methods of 2FA

Fingerprint
(something you are)

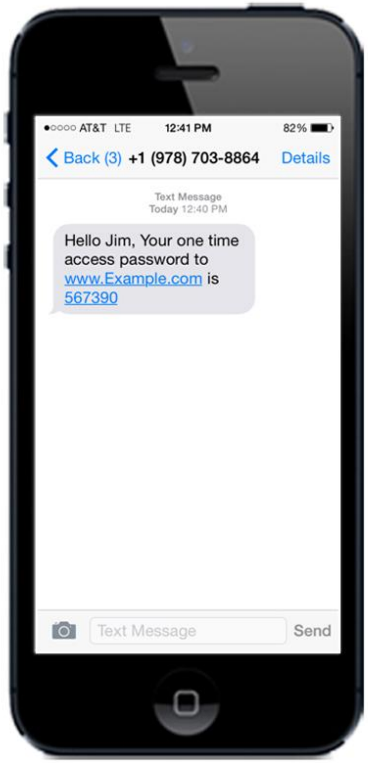


Grant access for “falk”

Touch ID for “SecSign”

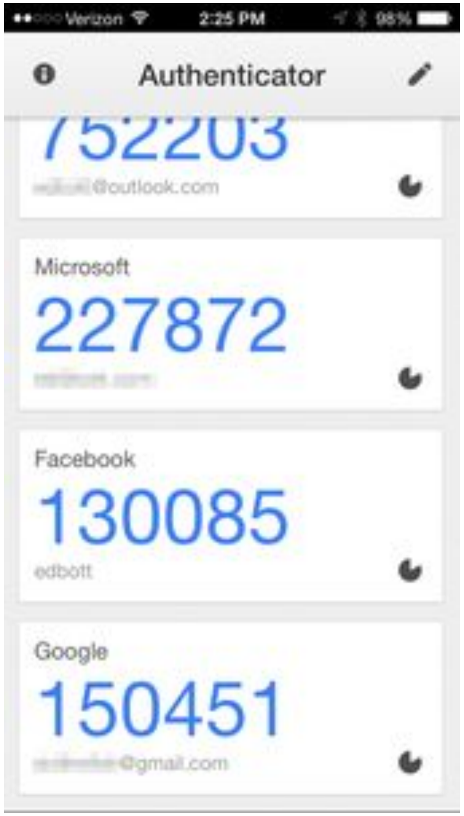
Authenticate for server login

SMS
(something you have)



Hello Jim, Your one time access password to www.Example.com is 567390

Authenticator app
(something you have)



752203
@outlook.com

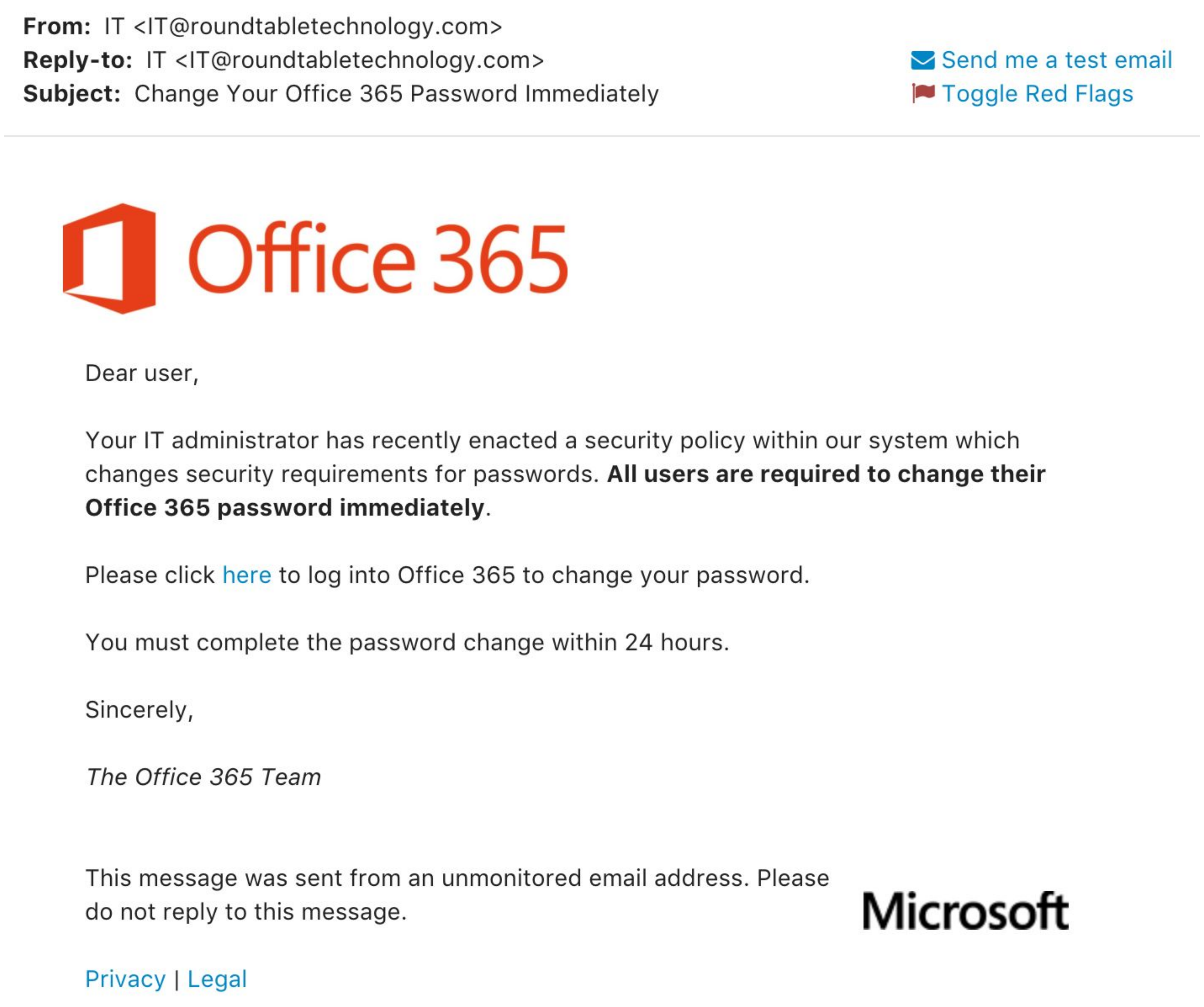
Microsoft
227872

Facebook
130085
edbott

Google
150451
@gmail.com

Phish or not a Phish?
#2

RoundTable TECHNOLOGY



From: IT <IT@roundtabletechnology.com>
Reply-to: IT <IT@roundtabletechnology.com>
Subject: Change Your Office 365 Password Immediately

Office 365

Dear user,

Your IT administrator has recently enacted a security policy within our system which changes security requirements for passwords. **All users are required to change their Office 365 password immediately**.

Please click here to log into Office 365 to change your password.

You must complete the password change within 24 hours.

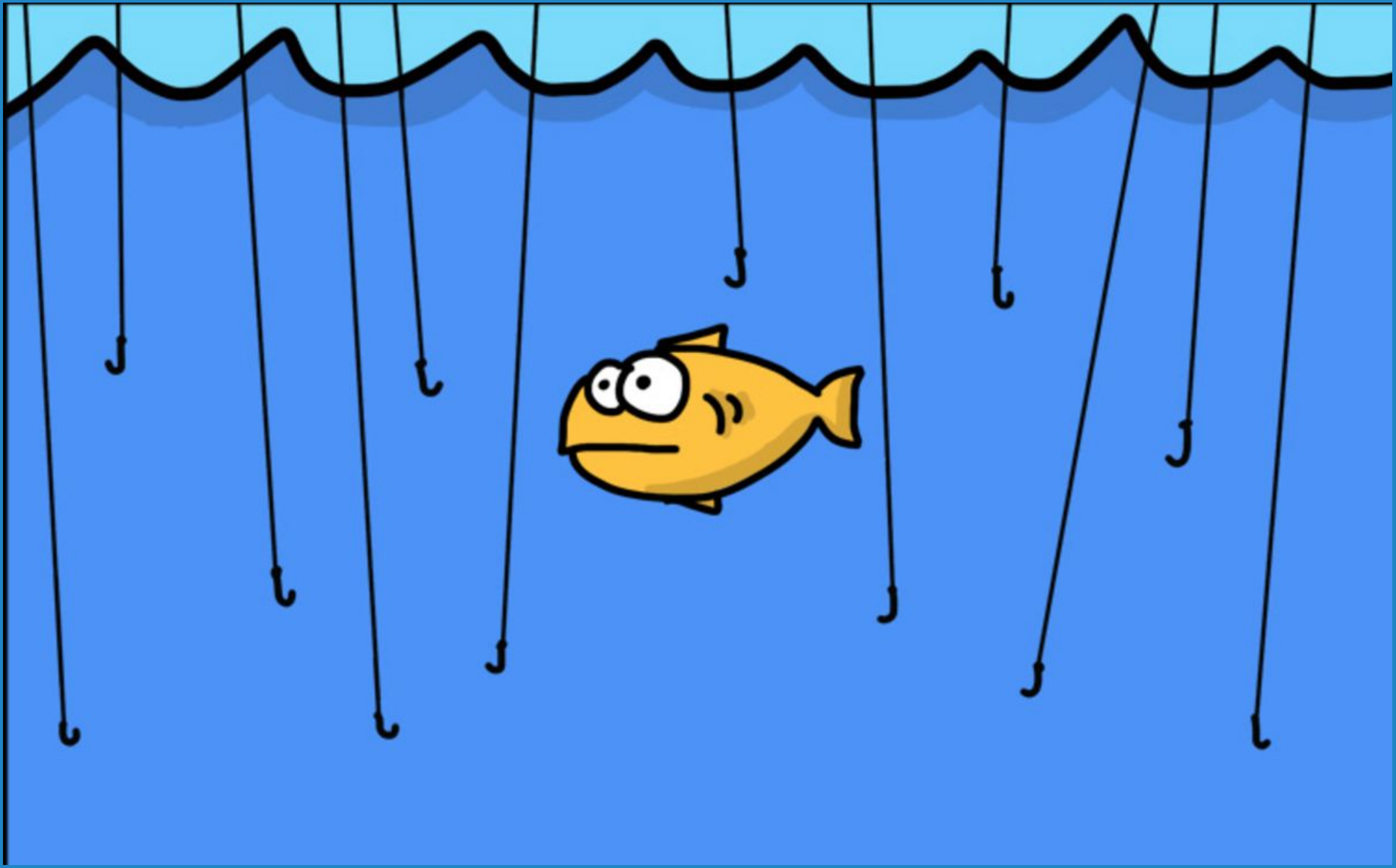
Sincerely,

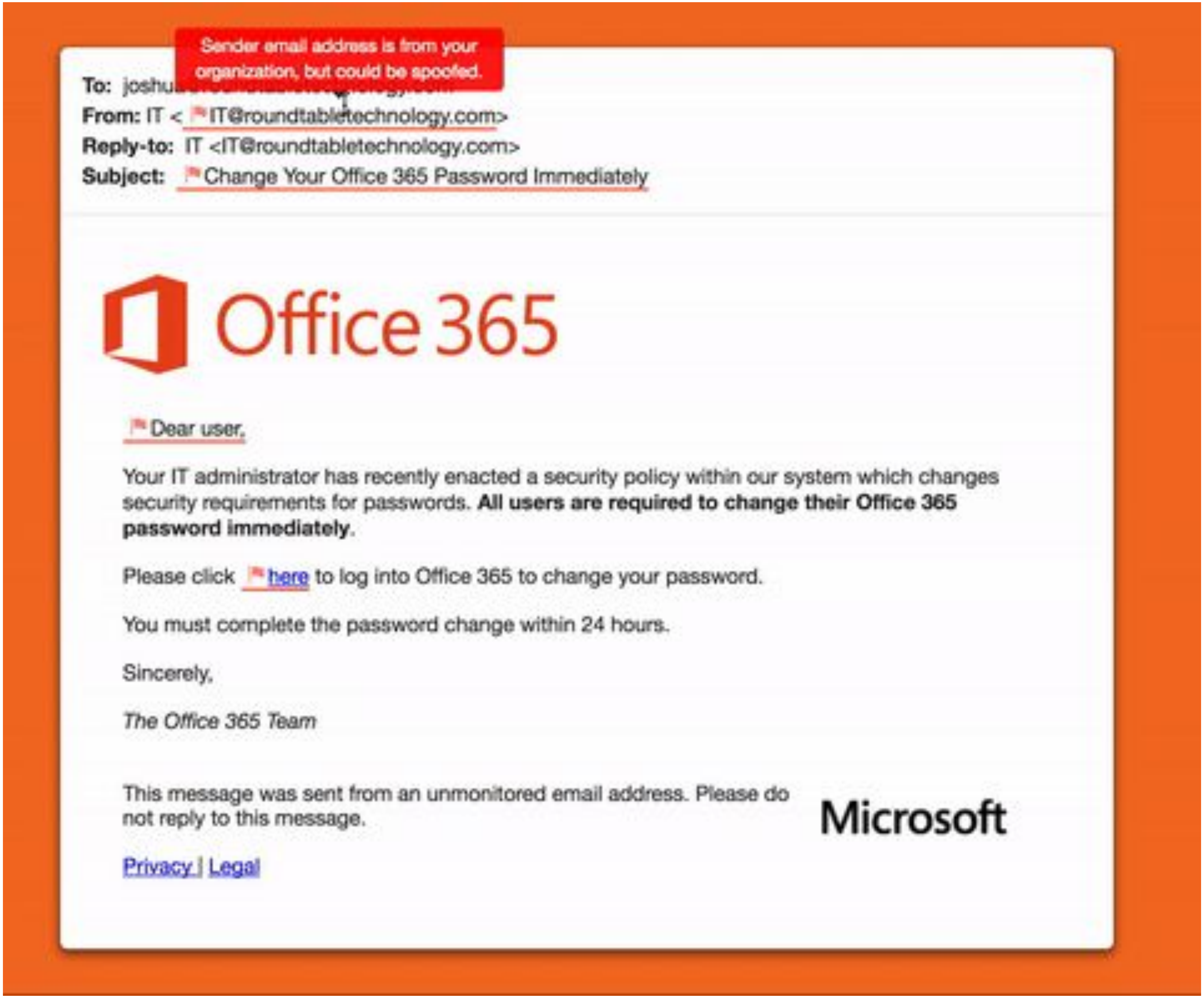
The Office 365 Team

This message was sent from an unmonitored email address. Please do not reply to this message.

Microsoft

Privacy | Legal





Sender email address is from your organization, but could be spoofed.

To: joshu

From: IT < 🚩IT@roundtabletechnology.com>

Reply-to: IT <IT@roundtabletechnology.com>

Subject: 🚩Change Your Office 365 Password Immediately

🚩Dear user,

Your IT administrator has recently enacted a security policy within our system which changes security requirements for passwords. **All users are required to change their Office 365 password immediately**.

Please click 🚩here to log into Office 365 to change your password.

You must complete the password change within 24 hours.

Sincerely,

The Office 365 Team

This message was sent from an unmonitored email address. Please do not reply to this message.

Privacy | Legal

Shadow IT

Risks with Mobile Technology

I'LL TAKE A TALL LATTE, A PUMPKIN SCONE, AND THE LOGIN CREDENTIALS OF EVERYONE ON YOUR WI-FI NETWORK.

Remote and Travel

If you do all the other things we have talked about
(and are going to talk about), you are already much safer.

These same practices make remote work and travel much safer.

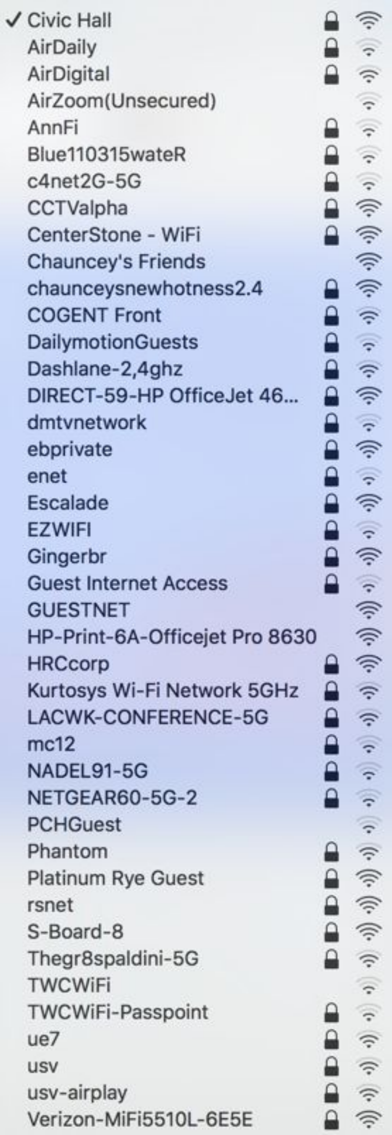
- Multi-Factor Authentication
- Device Encryption
- Using Virtual Private Networking
- Environmental Awareness
- Log out of sessions

Mobile Devices

- Protect your device with a STRONG password
  - (hint) 1234 is not a strong password
  - (hint) The letter Z on a pattern lock is not a strong password
- Encrypt your devices
- Learn how to disable services (bluetooth, wifi, location)
  - Consider disabling these when not needed

Wireless Networks

- Secure your own home WiFi with WPA2
- Avoid using public wi-fi
- When using public wi-fi, use a VPN
- Restrict sensitive transactions on unknown
- Tether instead of wi-fi if not cost-prohibitive



```
✓ Civic Hall                        🔒
  AirDaily                          🔒
  AirDigital                        🔒
  AirZoom(Unsecured)
  AnnFi                             🔒
  Blue110315wateR                   🔒
  c4net2G-5G                        🔒
  CCTValpha                         🔒
  CenterStone - WiFi                🔒
  Chauncey's Friends
  chaunceysnewhotness2.4            🔒
  COGENT Front                      🔒
  DailymotionGuests                 🔒
  Dashlane-2,4ghz                   🔒
  DIRECT-59-HP OfficeJet 46...      🔒
  dmtvnetwork                       🔒
  ebprivate                         🔒
  enet                              🔒
  Escalade                          🔒
  EZWIFI                            🔒
  Gingerbr                          🔒
  Guest Internet Access             🔒
  GUESTNET
  HP-Print-6A-Officejet Pro 8630
  HRCcorp                           🔒
  Kurtosys Wi-Fi Network 5GHz       🔒
  LACWK-CONFERENCE-5G               🔒
  mc12                              🔒
  NADEL91-5G                        🔒
  NETGEAR60-5G-2                    🔒
  PCHGuest
  Phantom                           🔒
  Platinum Rye Guest                🔒
  rsnet                             🔒
  S-Board-8                         🔒
  Thegr8spaldini-5G                 🔒
  TWCWiFi
  TWCWiFi-Passpoint                 🔒
  ue7                               🔒
  usv                               🔒
  usv-airplay                       🔒
  Verizon-MiFi5510L-6E5E            🔒
```

Key Term

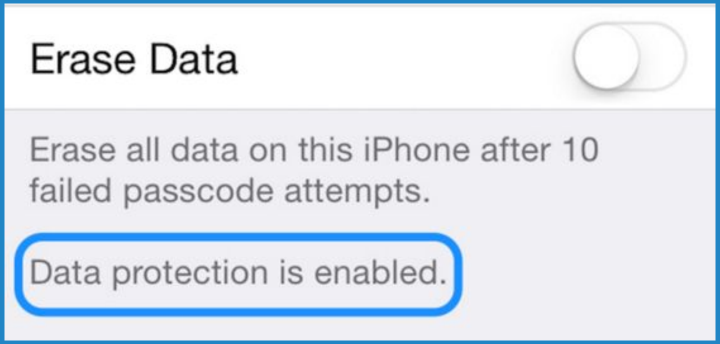
Encryption

Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

Unencrypted data is called plain text ; encrypted data is referred to as cipher text.

Encrypt Your Devices

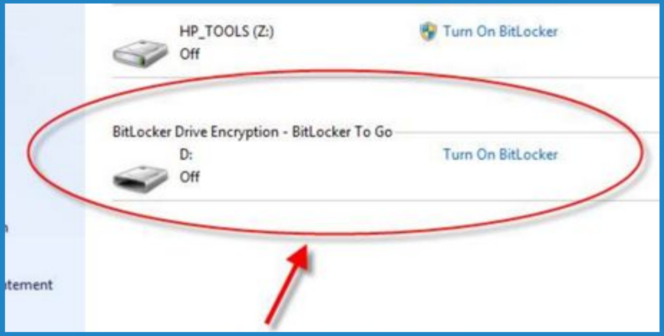
Encryption your laptop, smartphone and tablet is usually as easy as toggling a switch and creating a PIN or passkey.



Erase Data ○

Erase all data on this iPhone after 10 failed passcode attempts.

Data protection is enabled.



HP_TOOLS (Z:)
Off
Turn On BitLocker

BitLocker Drive Encryption - BitLocker To Go
D:
Off
Turn On BitLocker

on what you can do

- **Nurture** a Security Culture at your organization
- **Educate** yourself and others about tactics used to steal your info
- **Protect** your mobile devices and accounts with secure practices
- **Verify** any and all communications if you have any doubt

Going a step further…

Putting it all together for yourself

Cybersecurity Persona Template

Ricky the Activist

What needs protecting?

Hard drives, data files, research papers

Social media accounts

Correspondence with other activists

Government Sources

Over many years of hard work, Ricky has a substantial amount of content on his blog. He has many files full of research, plans and data that must be kept confidential - Integrity is everything in his line of work. Ricky is concerned that his information may be intercepted by foreign agencies who are not sympathetic to his cause.

Ricky is an activist and blogger who calls attention to humanitarian issues around the world. Ricky's work is constantly under scrutiny by various organizations and his online accounts are regularly watched and susceptible to hacking and interception.

Due to rising safety concerns, Ricky is considering **encryption of all data and communications** with his team.

To mitigate these vulnerabilities:

Ricky uses a **Virtual Private Network (VPN)** to access the internet securely when connecting to wi-fi in public places.

Ricky **encrypts** all of his email communications.

All of his online accounts use **Two-Factor Authentication (2FA)**

Ricky **encrypts all sensitive files, hard drives and external media.**

Ricky creates **strong, 30-character+ passwords** with special characters and numbers organized by a **password manager.**

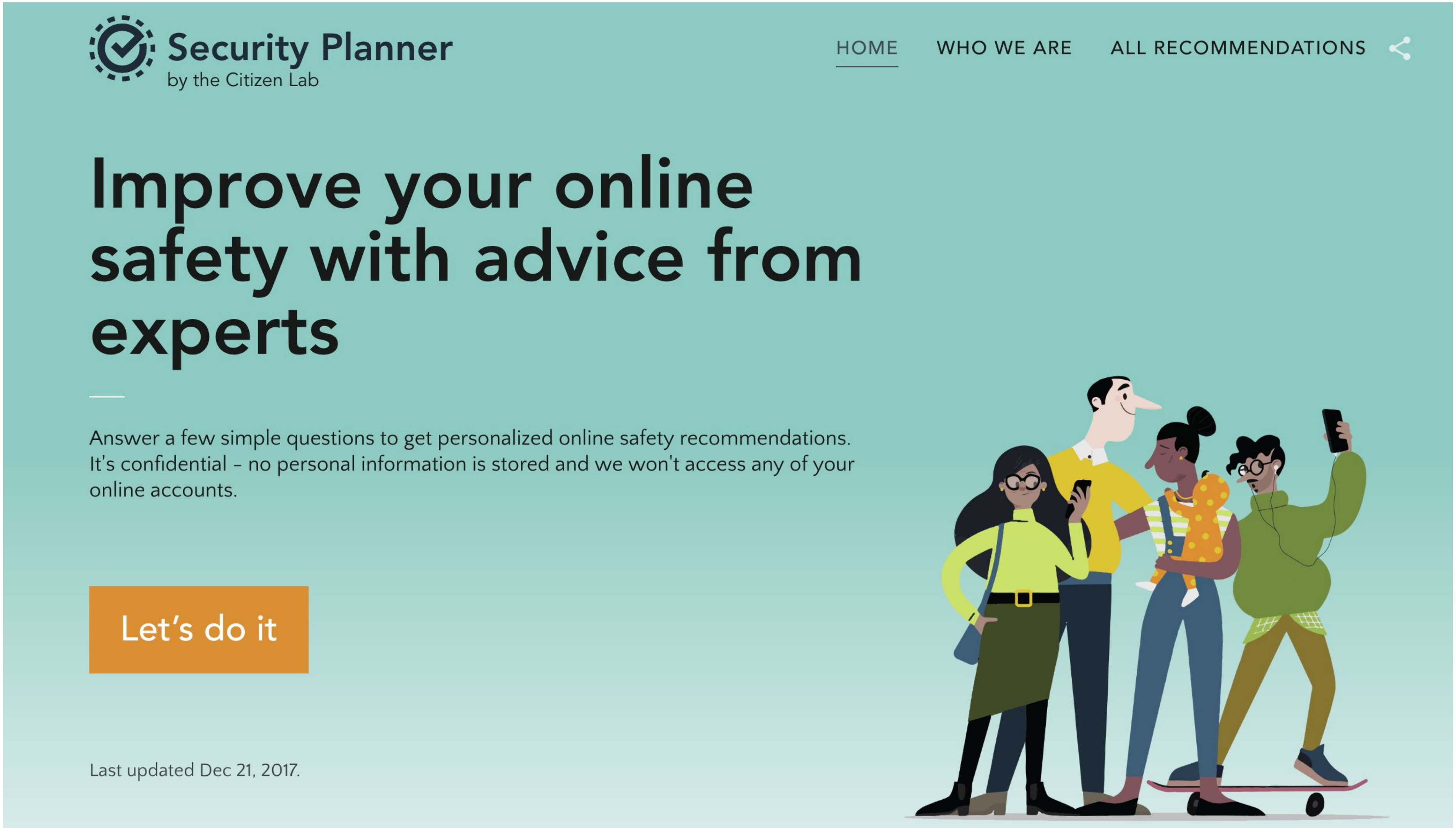
Ricky **regularly clears out his chat history** to prevent previous communications falling into the wrong hands.

Original Source: https://www.accessnow.org/cms/assets/uploads/2017/02/A-first-look-at-digital-security_DigiCopy.pdf

Cybersecurity Persona Template

What needs protecting?

To mitigate these vulnerabilities:



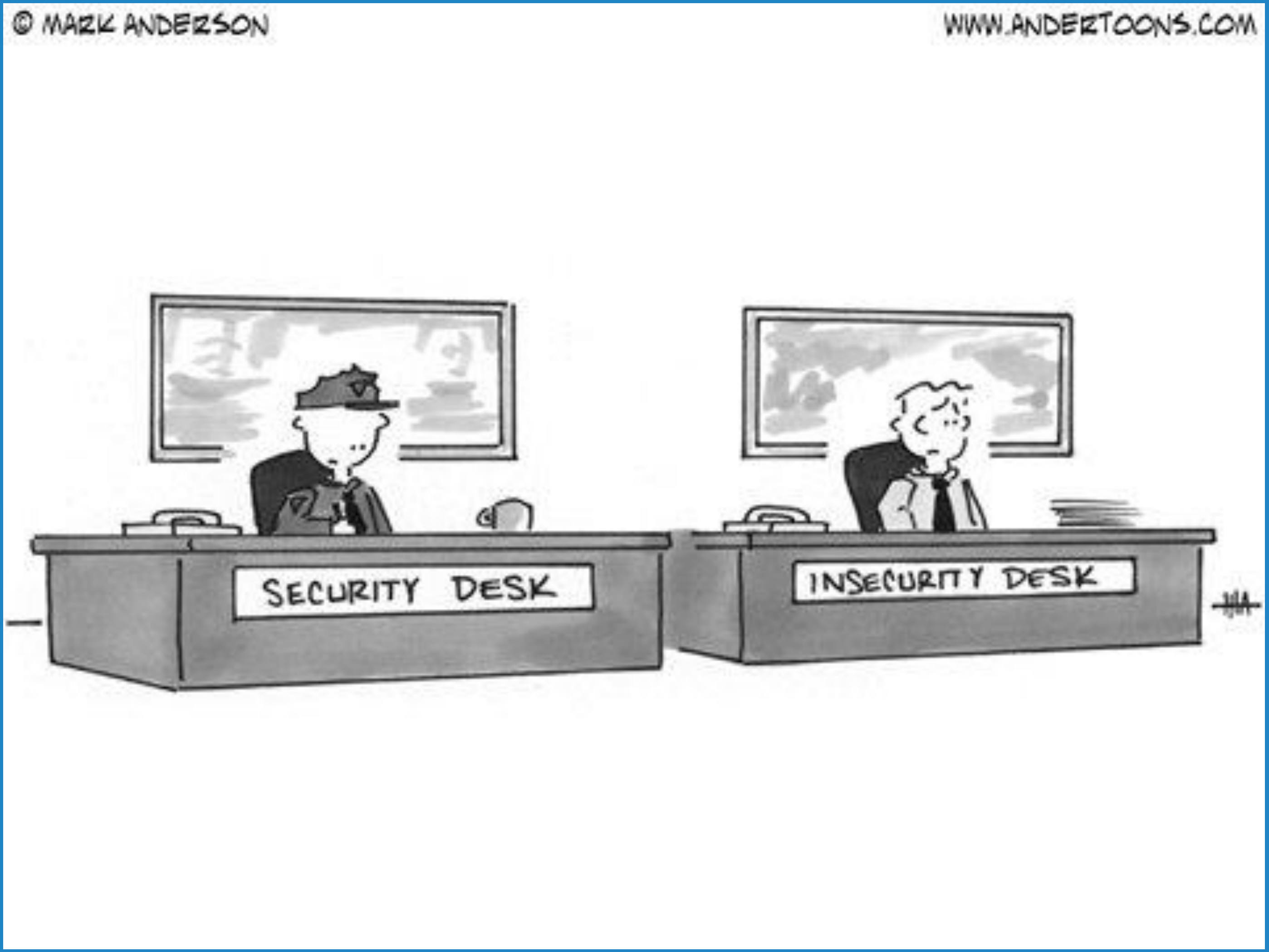
Improve your online safety with advice from experts

Answer a few simple questions to get personalized online safety recommendations. It's confidential - no personal information is stored and we won't access any of your online accounts.

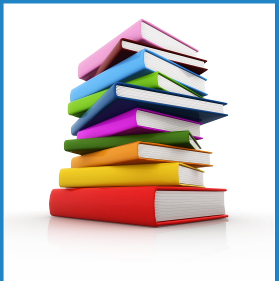
Last updated Dec 21, 2017.

Now tell us again, at which desk do you feel like you belong?

TAKE
2


© MARK ANDERSON
WWW.ANDERTOONS.COM
SECURITY DESK
INSECURITY DESK

Q.
A.



Resources

- Access Now - First Look at Digital Security
- Carnegie Mellon Phishing Education
- OpenDNS Phishing Quiz
- Today.com - Not Bad Phishing Quiz
- Sonicwall Email Phishing Quiz
- FTC - Scam Alerts
- FTC - About Phone Scams
- More Free Security Resources from RoundTable
- And of course, ninja.rtt.nyc (our Cybersecurity Ninja Series)

Parking Lot.