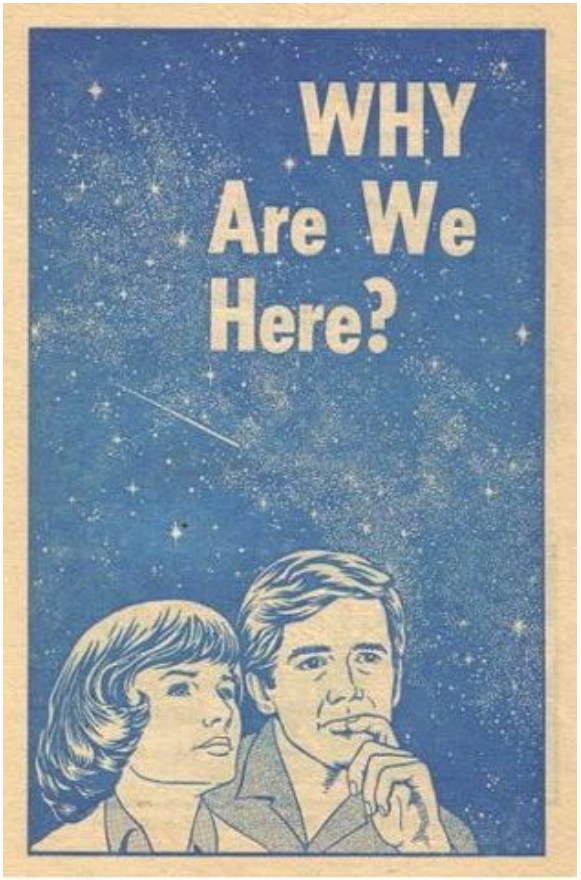
Cybersecurity Awareness Training

Immigration Advocates NETWORK

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.

What we'll cover today

- What is cybersecurity?
- Why do we care about it?
- What we can do about it
- Next steps

There are things you can do that can 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!

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

Cybersecurity

Key Term

IBM

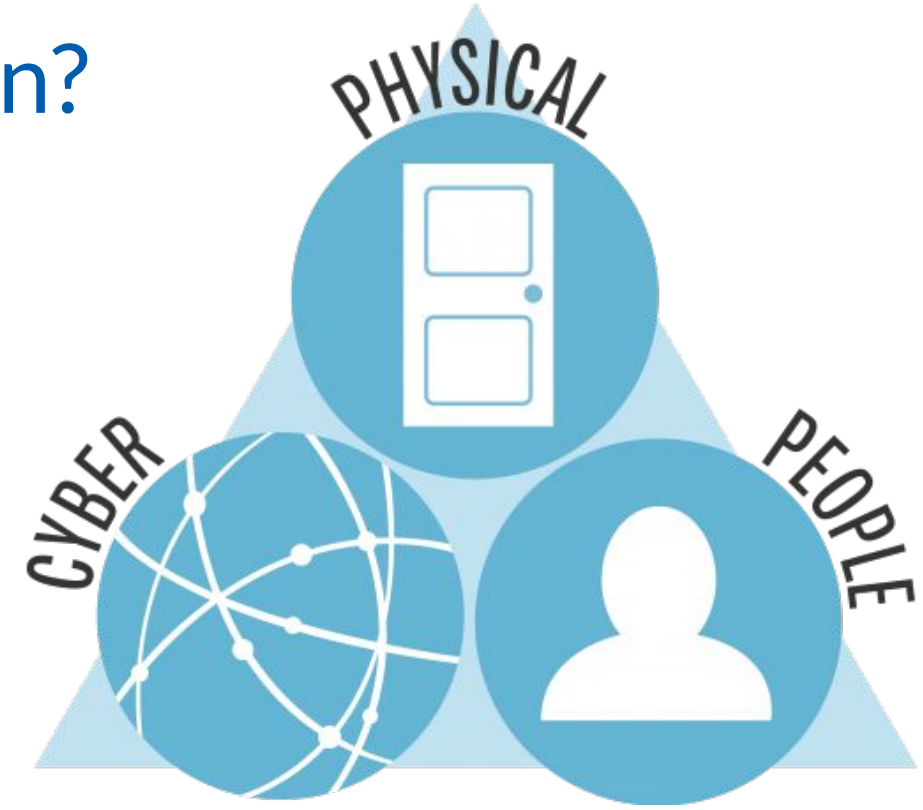
IBM's Definition . . .

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

Security Triad

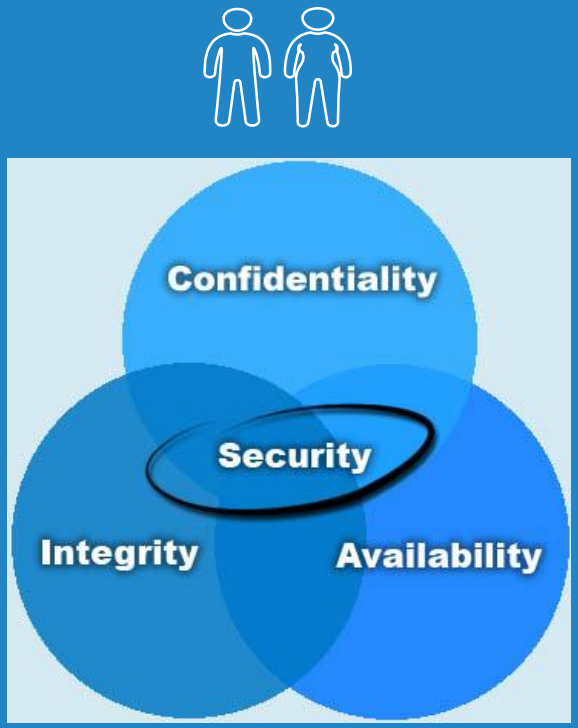
Where do people fit in?

Everywhere



The CIA Security Triad

(yes another triad)

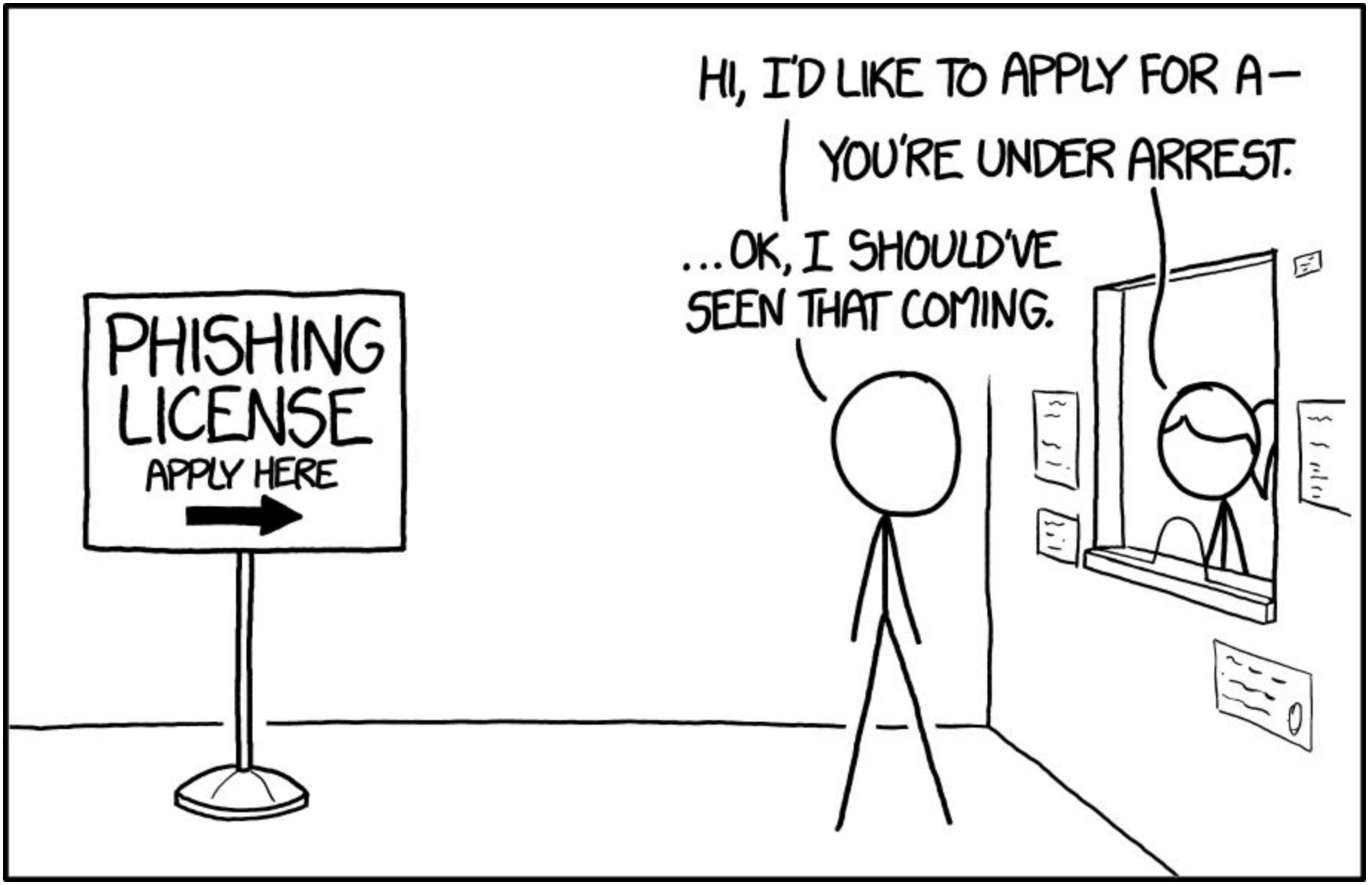


C - How bad would it be if the information was exposed

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

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

Congratulations!
You made it through three slides of boring stuff


PHISHING LICENSE
APPLY HERE
HI, I'D LIKE TO APPLY FOR A—
...OK, I SHOULD'VE SEEN THAT COMING.
YOU'RE UNDER ARREST.

Phishing

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)

Phish or not a Phish?

#1

Phish or not a Phish?

#1

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

AmericanAirlines
AA.com

Home | Login | My Account | Worldwide Sites | Contact AA | FAQ | Search... | GO

AA.com

Reservations
Travel Information
Net SAAver & Special Offers℠
AAdvantage®
Products & Gifts
Business Programs & Agency Reference
About Us

Deal Finder™
Get Details

Login

ESPAÑOL

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 GO

Enroll in the AAdvantage Program - It's Free!

DealFinder™ | RSS | AA.com en Español

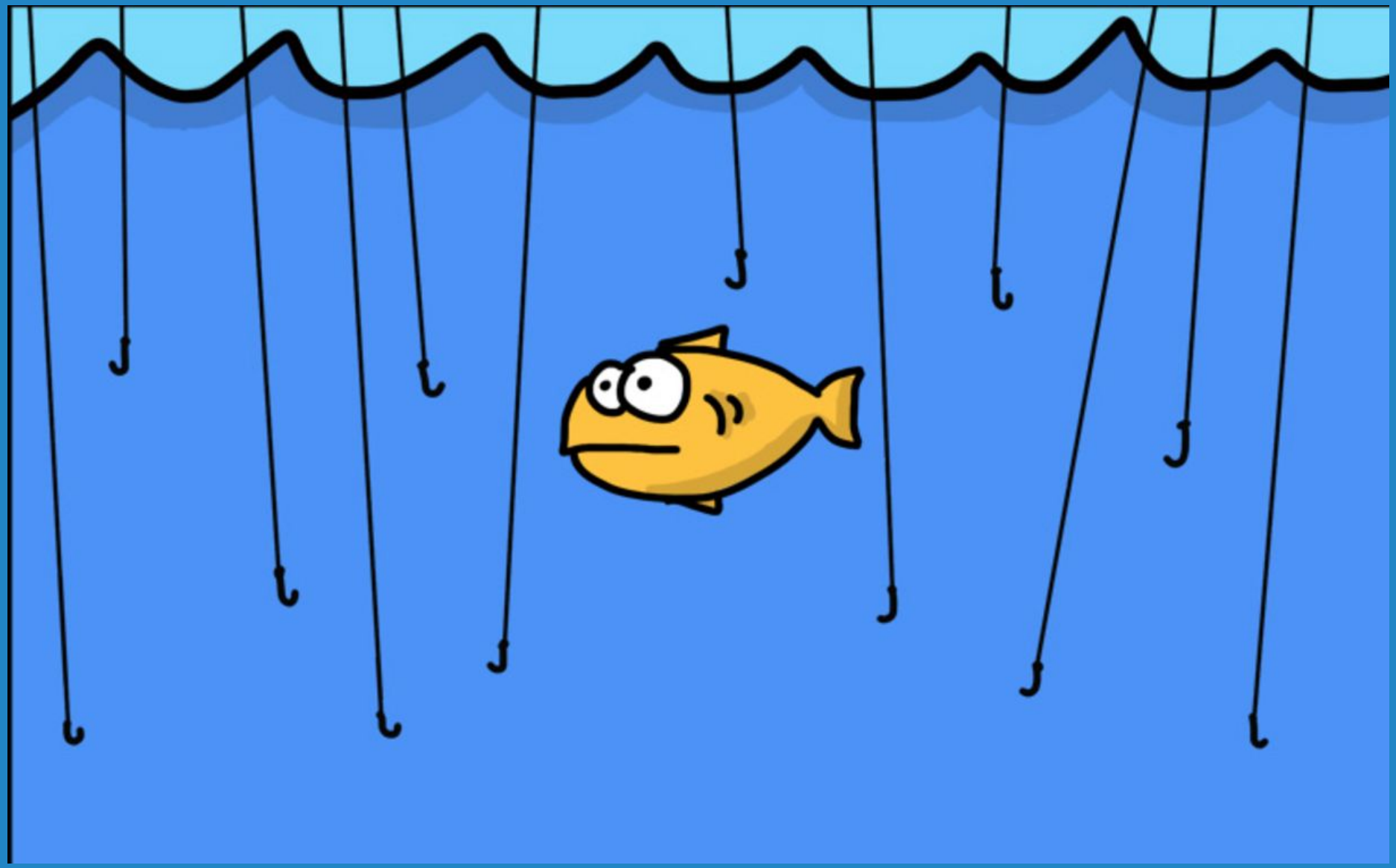
Airline Tickets | AA Careers | Copyright | Legal | PRIVACY POLICY | Customer Service Plan | Browser Compatibility | Site Map

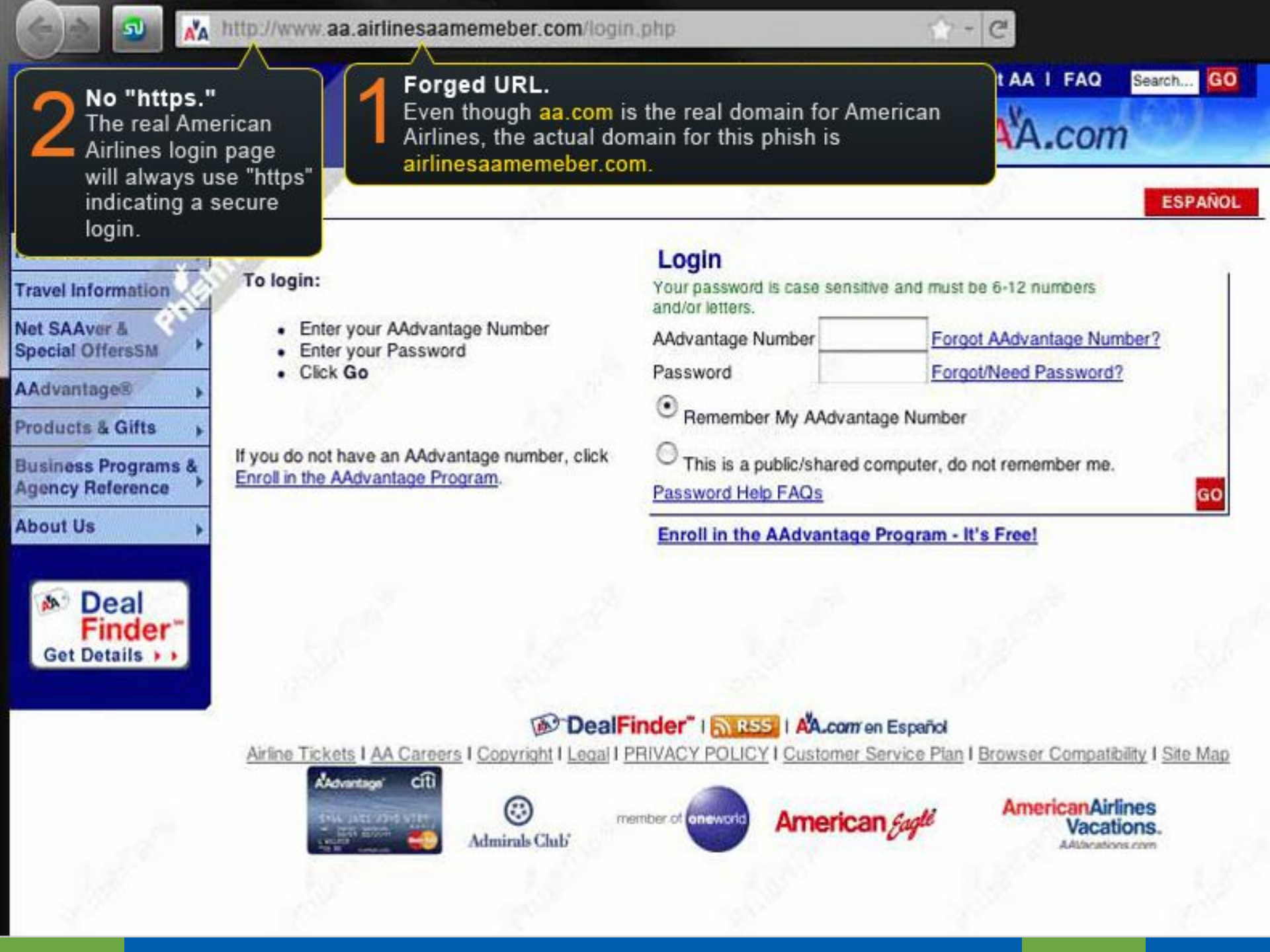
Admirals Club

member of oneworld

American Eagle

American Airlines Vacations
AAVacations.com




http://www.aa.airlinesaamemeber.com/login.php
2 No "https."
The real American Airlines login page will always use "https" indicating a secure login.
1 Forged URL.
Even though aa.com is the real domain for American Airlines, the actual domain for this phish is airlinesaamemeber.com.
t AA I FAQ
Search...
GO
A.com
ESPAÑOL
Travel Information
Net SAAver & Special Offers℠
AAdvantage®
Products & Gifts
Business Programs & Agency Reference
About Us
Deal Finder™
Get Details
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
GO
Enroll in the AAdvantage Program - It's Free!
DealFinder™ I RSS I AA.com en Español
Airline Tickets I AA Careers I Copyright I Legal I PRIVACY POLICY I Customer Service Plan I Browser Compatibility I Site Map
AAdvantage citi
Admirals Club
member of oneworld
American Eagle
American Airlines Vacations

The Threat Model we all have in common

The Three P's of Sensitive Information

PCI - Payment Card Industry (regulated by PCI-DSS)

- Credit Cards

PHI - Protected Health Information (regulated by HIPAA)

- Medical Records
- Billing Information
- Health Insurance Information
- Any individually identifiable health information

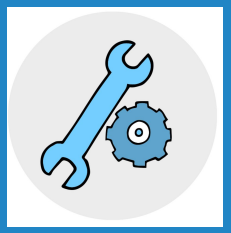
PII - Personally Identifying Information (not regulated)

- Social Security Number (SSN)
- Passport Number
- Driver's License Number
- Individual Taxpayer Identification Number (ITIN)
- Alien Registration Number (A-Number)

Additional Threat Modeling

Some questions to ask:

- Who might want to disrupt our work?
- Who might want access to our information?
- What would be their most likely targets?
  - Our website?
  - Our people?
  - Our information?
  - Our money (it's usually money)
- How motivated are they?
- How capable are they?



How?

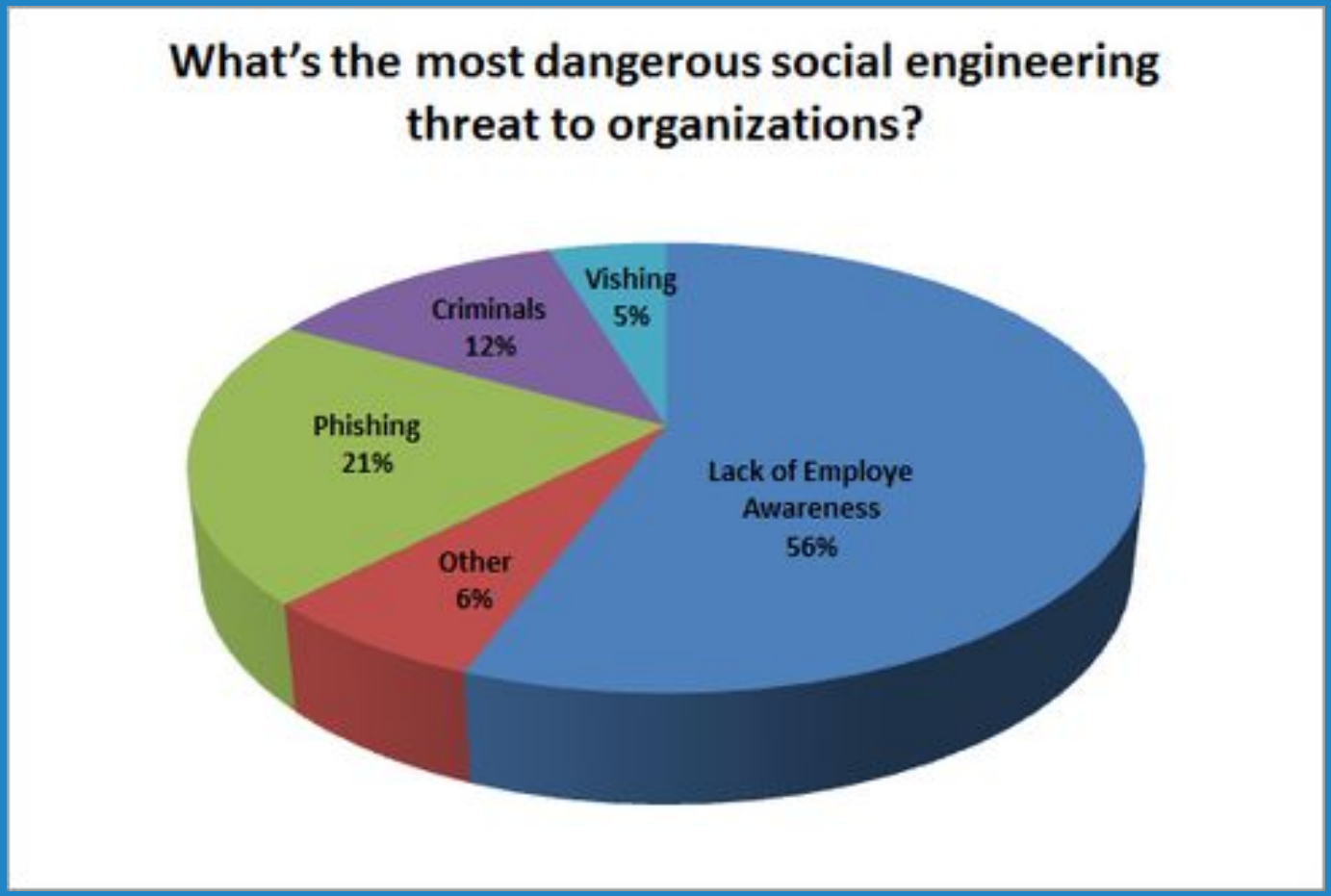
- Phishing
- Social Engineering
- Malware
- Theft
- Error
- Dumpster Diving
- Exploiting Vulnerabilities

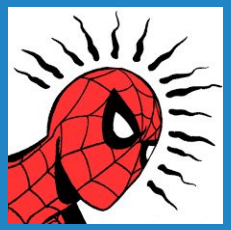
Social Engineering

Key Term

The manipulation of our human instinct to help

Social Engineering





7 Things to Get your Spidey Sense Tingling

- Initiation
- Urgency
- Fear
- Authority
- Money
- Credentials
- Information

Book recommendation - Gift of Fear by Gavin DeBecker

Spear Phish

From: Evan Desjardins (evan@roundtabletechnology.com
Sent: Thursday, May 19, 2016 2:15 PM
To: Ben Gardner
Subject: Wire Request

Hello Ben,

I have an outgoing domestic wire transfer i want you to process for me today. What details do you need to process this to hit the recipient account today?

Thanks,

Evan Desjardins

President, RoundTable Technology

Phish or not a Phish?
#2

Phish or not a Phish?
#2

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.

Consolidated Edison Company... (US) https://apps.coned.com/cemyaccount/NonMemberPages/Login.aspx?la

Search

conEdison

My Account | Energy & Information | Safety & Outages | Business Resources | Investors | About Us

- conEd.com home
- my account home
- start service
- My Energy Toolkit
- Commercial Energy Calculator
- help

my account

Welcome to Con Edison's My Account service center, where you can quickly and conveniently pay your bill online, view account information, submit a meter reading and view past bills without waiting and much more.

Log In to My Account

On My Account you can pay your bill, check your balance, enroll in paperless billing, special services and more. No waiting!

* Indicates required fields

* **Username:**

Forgot username?

* **Password:**

Forgot password?

Remember my username | Sign In

Help

Steam customers, click here.

Are you a new user?

Click 'Register Now' to create your username and password to access this secure application.

It's quick and easy to manage your Con Edison account online all year!

Register Now

Why Register?

Help

Si prefiere ver el sitio en español, haga clic en la casilla que aparece más abajo.

español

REPORT ELECTRIC SERVICE PROBLEM
Click Here

CHECK SERVICE PROBLEM STATUS
Click Here

CLAIMS INFORMATION
Click Here

START SERVICE
Click Here

VIEW YOUR STEAM BILL ONLINE
Click Here

Not a Phish

123456 is not the best password

From Ashley Madison breach

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

From LinkedIn breach

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

The best passwords are long, complex and random alphanumeric strings.

Such as

7!G2Kq@qyhTfTTQIwlcd82Kt

Or

yHlQHtLp7YoAb^&ib3ZHJt4WP#xCuBZEO3S7tIle%lhUb7b81

Or

I like to eat donuts on Wednesdays.

Notice anything different about the last one?

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

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

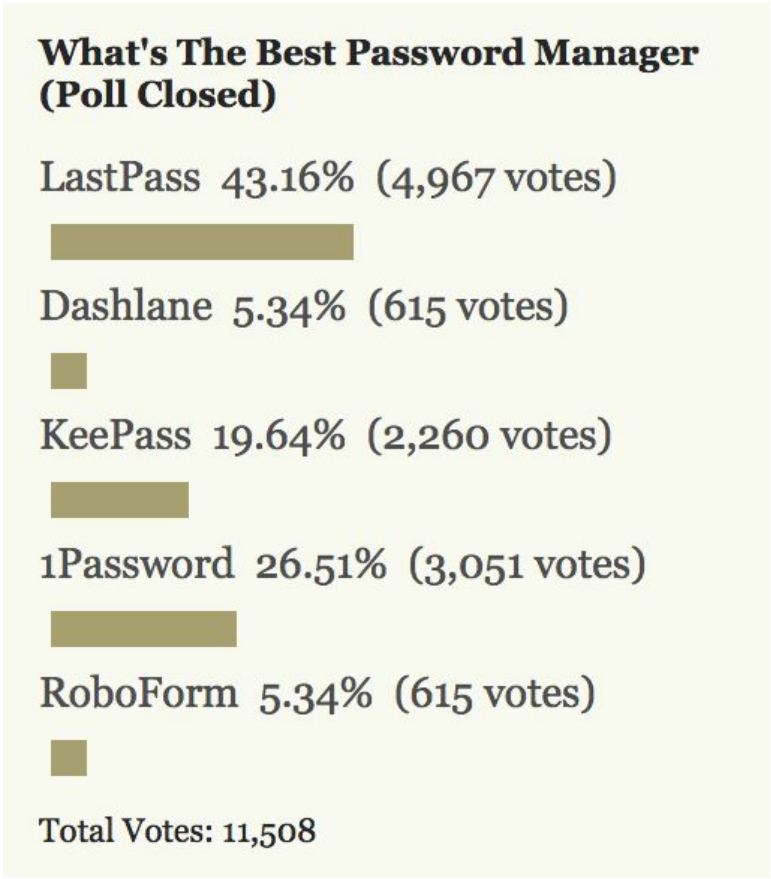
LastPass

1Password

KeePass

dashlane

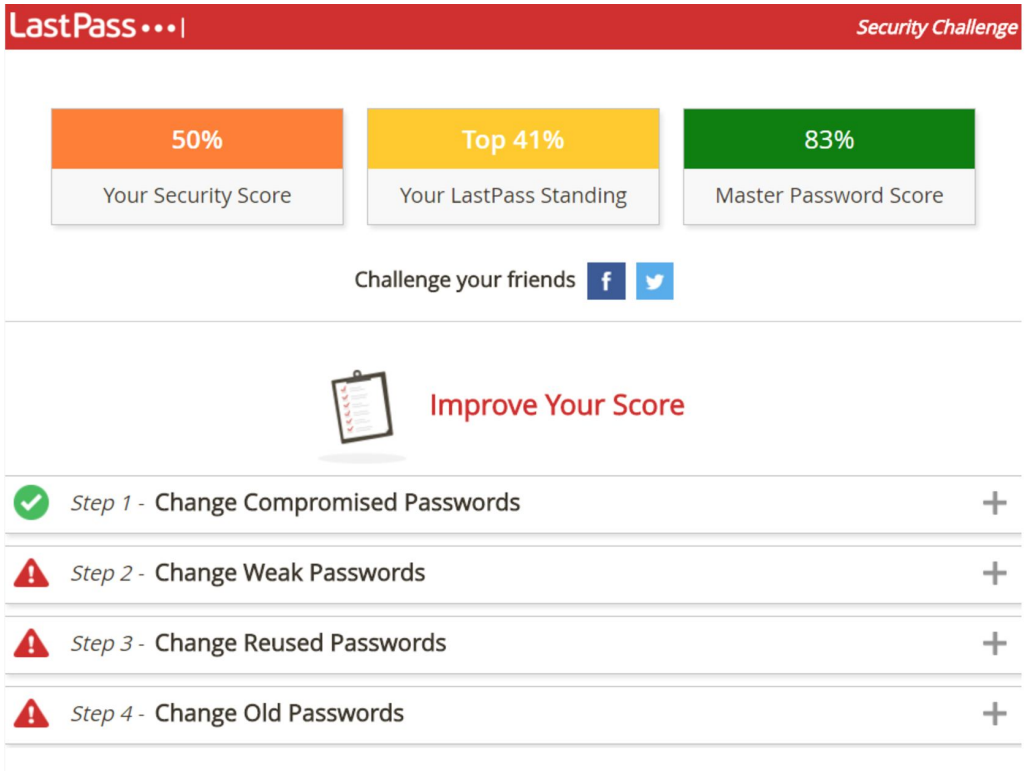
RoboForm



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



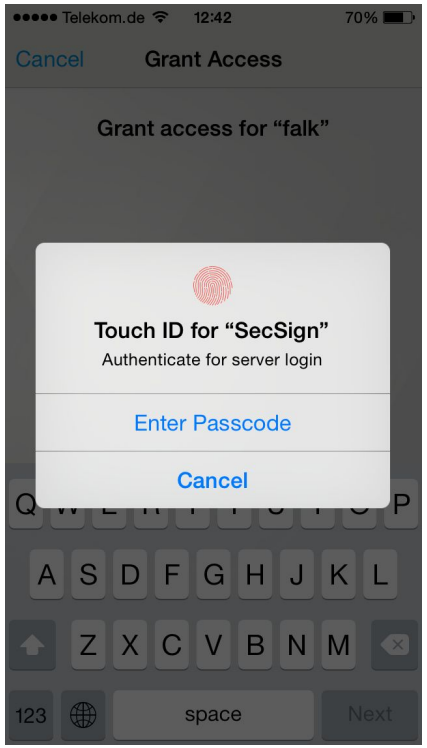
Ways to Authenticate

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

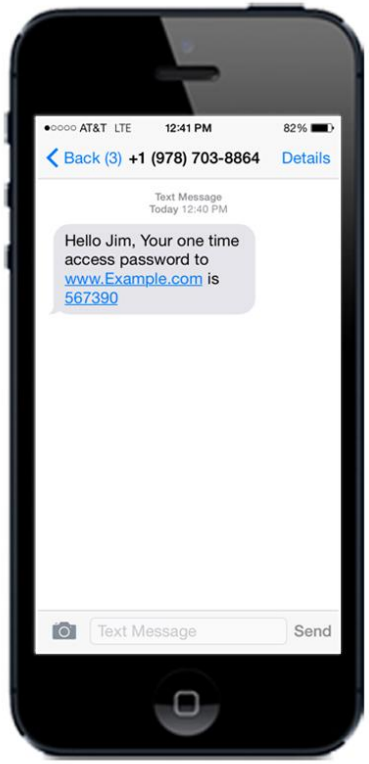
A form of 2FA we all use already

Common Methods of 2FA

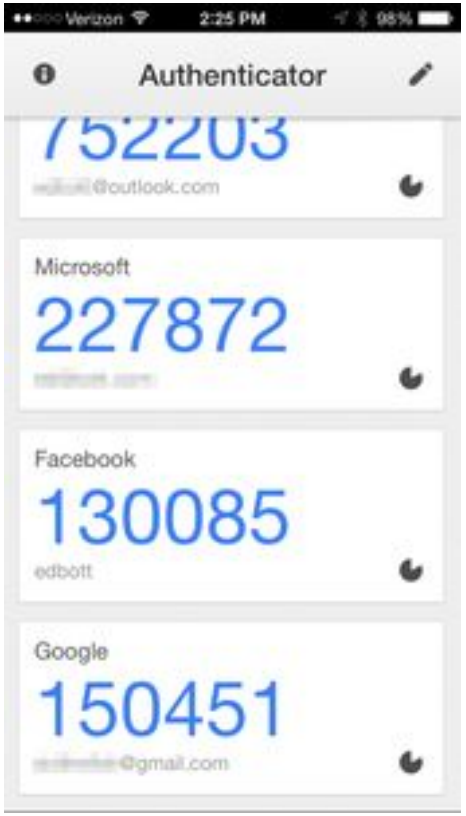
Fingerprint
(something you are)



SMS
(something you have)



Authenticator app
(something you have)



Phish or not a Phish?
#3

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

Send me a test email
Toggle Red Flags

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.

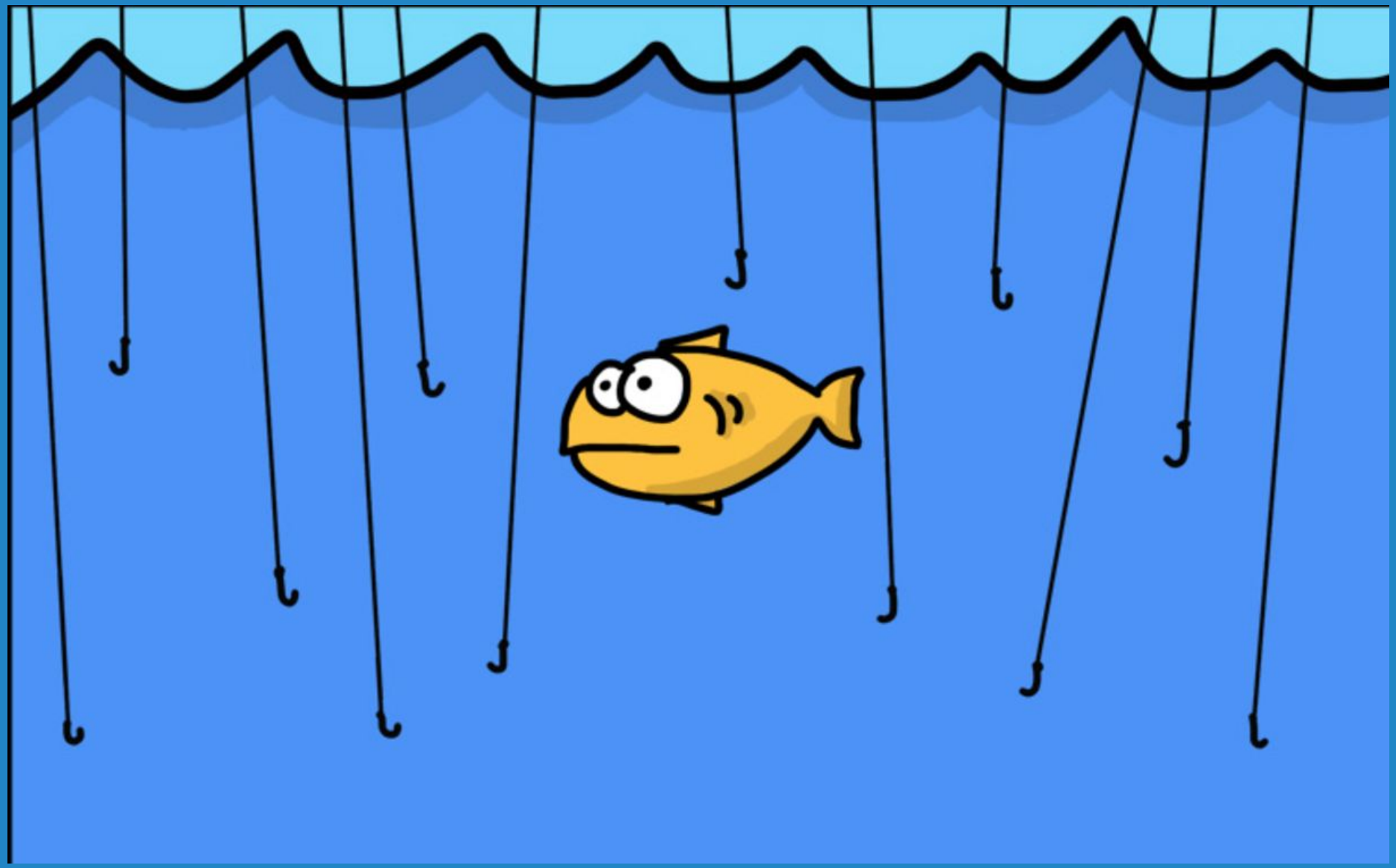
Sincerely,

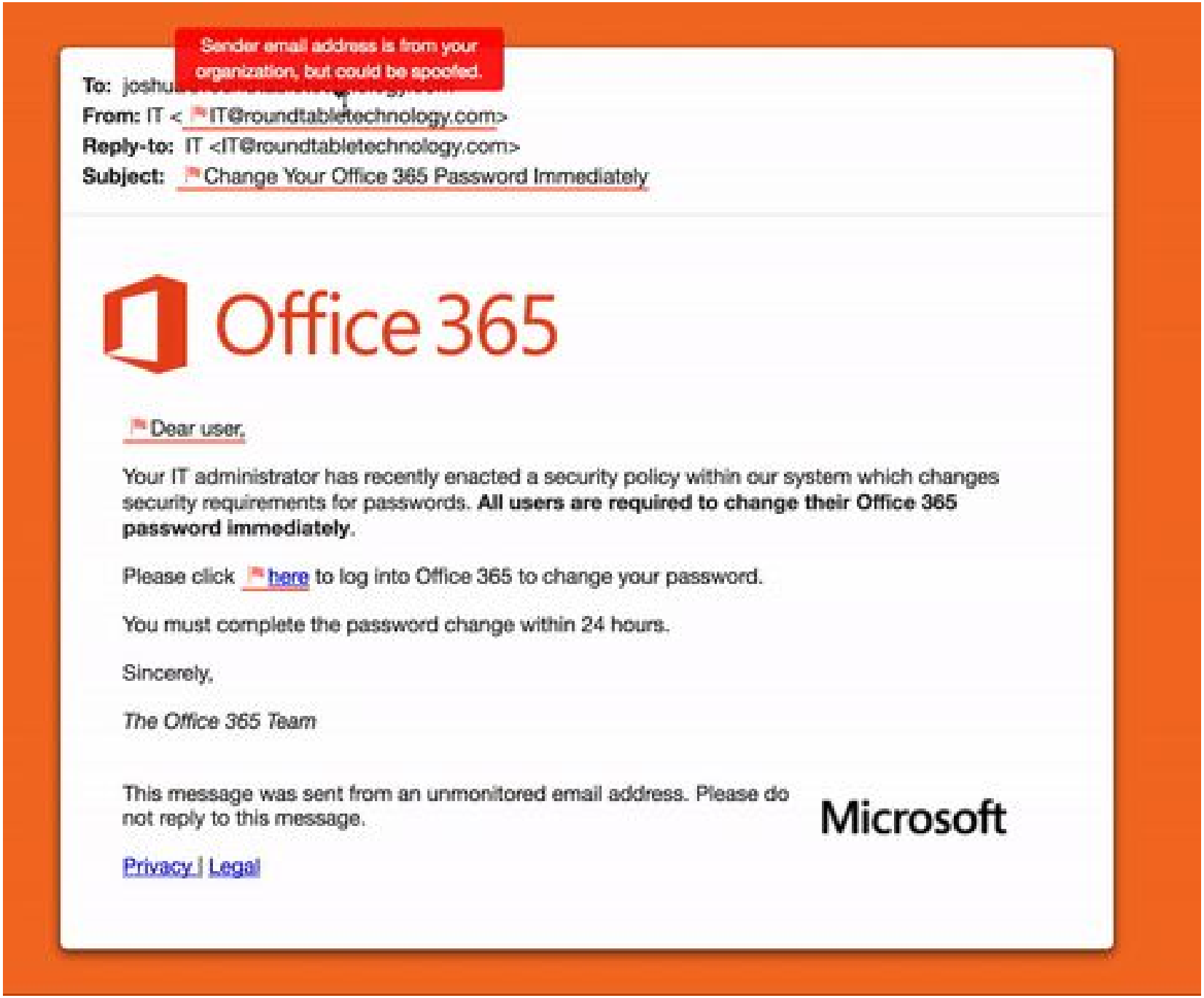
The Office 365 Team

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:
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

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

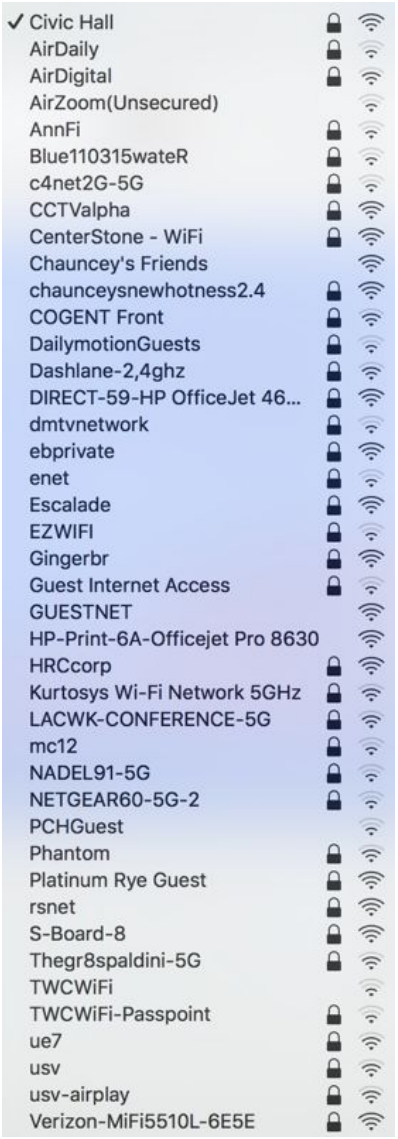
And it doesn't hurt to keep your eyes on your stuff!

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 data
- Keep eyes on them
- Enable FindYourPhone
- 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 wi-fi
- Tether instead of wi-fi if not cost-prohibitive



Key Term

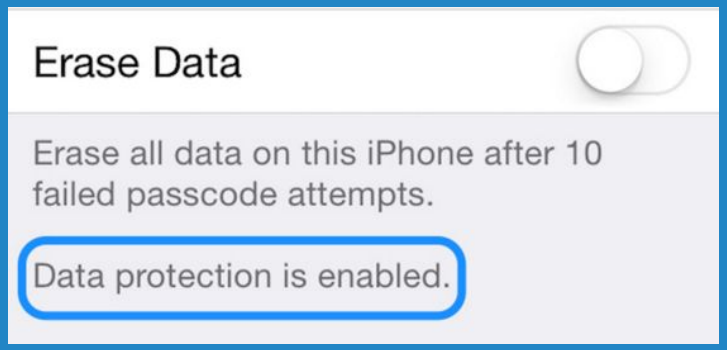
Encryption

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.

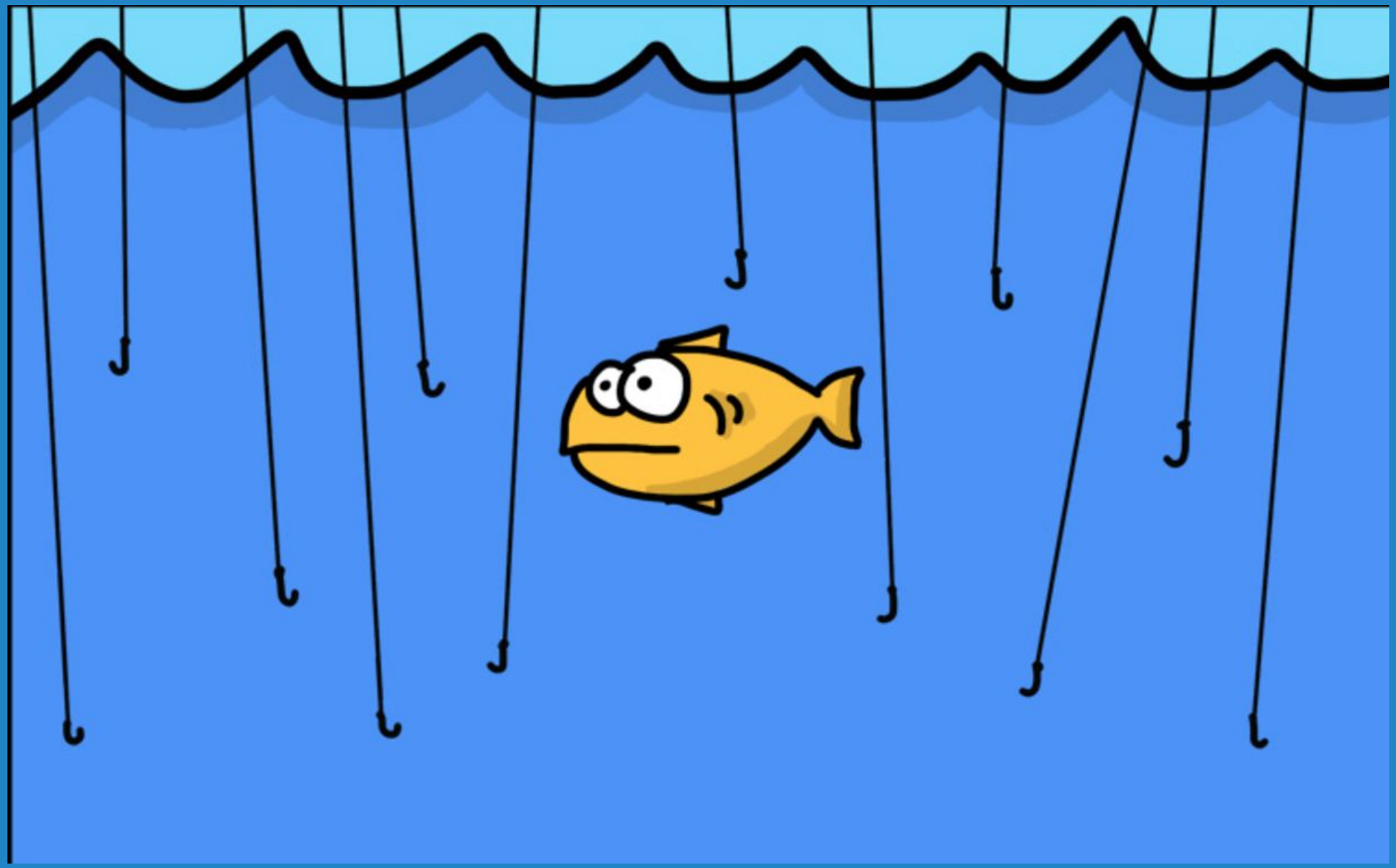
Encrypt Your Devices

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



Phinal Phish!


http://twitter.com.all09.info/fun_en/
twitter
Search
Username or email
Password
Forgot?
Remember me
Sign In
If you've been using Twitter from your phone, click here to sign up on the web.
Create Your Account
Join!
Already using Twitter from your phone? Click here.
Select Language ...
© 2011 Twitter About Us Contact Blog Status Resources API Business Help Jobs Terms Privacy



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 Legal Advocate & Blogger

Ricky is a legal advocate and blogger who often speaks out on behalf of immigrants in his community. Ricky and his organization are constantly targeted by anti-immigrant groups and their 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.

What needs protecting?

- Hard drives, data files, research papers
- Social media accounts
- Email correspondence
- Government Sources

Over many years of hard work, Ricky has a substantial amount of content on his blog. He also has many files full of research, plans and correspondence with local organizations, government, and allies that must be kept confidential. Ricky is concerned that his information may be intercepted by anti-immigrant groups or others.

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.

Cybersecurity Persona Template

What needs protecting?

To mitigate these vulnerabilities:

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

Resources

- Access Now - First Look at Digital Security
- Carnegie Mellon Phishing Education
- OpenDNS Phishing Quiz
- Sonicwall Email Phishing Quiz
- Pew Research Cybersecurity Quiz
- FTC - Scam Alerts
- FTC - About Phone Scams
- More Free Security Resources from RoundTable


Q.
A.