Who is Chip Wentz?

- Principal, EY Advisory - Americas Data Protection and Privacy Cybersecurity Leader
- Cybersecurity professional for 20 years
- Work with organizations around the world on securing the company and people
- NC native, NCSU Alum

What my friends think I do

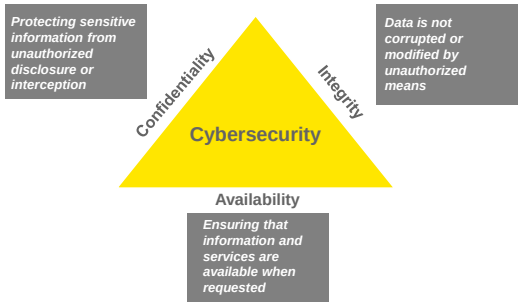
What my family thinks I do

What I really do

Our goals today

1. Share real-life examples of the cyber threat landscape
2. Share tactical recommendations that you can immediately perform at work and at home
3. Answer your questions

Cybersecurity is protecting information



Why is this important to me?

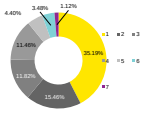
Data breach statistics

Data records are lost or stolen at the following frequency:

Every day	Every hour	Every minute	Every second
4,530,602 records	**188,775 records**	**3,146 records**	**52 records**

Data records stolen or lost by industry

Shows percentage of total records



Date range: 2013 - present

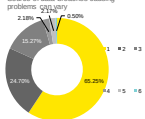
Number of breach incidents by type

Attackers use a variety of techniques against organizations

Date range: 2013 - present

Number of breach incidents by source

Source of data breaches causing problems can vary



Date range: 2013 - present

Source: http://breachlevelindex.com/

Can I see this data another way?

World's biggest data breaches
Selected losses greater than 30,000 records (as of 5 January 2017)

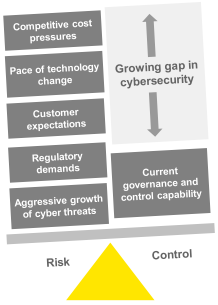
- River City Media: 1,370,000,000
- Friend Finder Network: 412,000,000
- MySpace: 164,000,000
- VK: 100,544,934
- Dailymotion: 85,200,000
- Weebly: 43,000,000
- Yahoo!: 32,000,000
- Mail.ru: 25,000,000

Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Cybersecurity
Is every company a target?

- Common misconception
  - "I don't process credit card transactions internally, therefore, my company is not a target."
- Reality
  - Companies can be targeted for many reasons:
    - Company is a vendor of the ultimate target
    - Research and development information
    - Clients' plans and specs
    - Sensitive merger and acquisition information
    - Disrupt operations

The reality of business today
Cybersecurity hot topics



Cyber risks are ever increasing in a world with *no boundaries* and *no rules*

- Growing regulatory and government focus
- Acute cost and competitive pressure
- Technology developing in leaps and bounds, especially as our clients move toward the "Internet of Things" (IOT)
- Increased erosion of perimeter from third parties, social media and personal devices
- Extended supply chain means links to smaller business partners
- Rising level and sophistication of external threats
- Risk outpacing organizations' ability to keep up

Where it all started

Who is Hilda Schrader Whitcher?

- SSN stolen over 40,000 times
- At the card's peak rate of use, almost 6,000 individuals were using her SSN number
- Used as late as 1977

Mrs. Whitcher compares the Social Security card "issued by Woolworth" with her own real card of the same number.

The card that started all the fuss!

- Source: https://www.ssa.gov/history/ssn/misused.html

Challenges – why are users the target?

- Lack of experience: We are experiencing a world we never grew up in.
- Lack of education: No one taught us how to stay safe on the internet.
- Always-on access: We have constant internet access through a variety of devices.

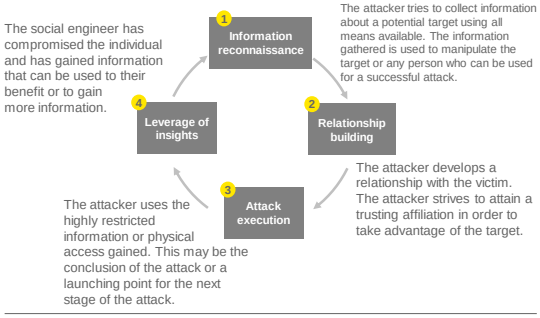
How does this happen?

One common entry vector that can lead to data breaches is social engineering

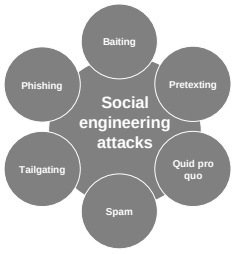
Social engineering definition: *The psychological manipulation of an individual to gain access to information.*

Social engineering is a component of most cyber attacks on individuals and companies.

How do social engineering attacks happen?



What are the types of social engineering attacks?

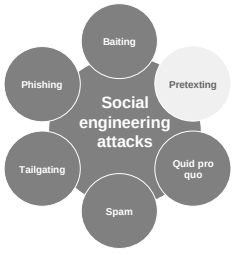


Types of social engineering attacks
Baiting

Baiting involves an attacker dangling something you want in order to entice you to take an action the criminal desires.

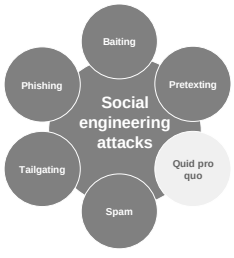
Example: A USB flash drive with a company logo was left out in the open. In order to assist in finding the owner, an employee plugged the USB drive into a laptop which then became infected with malicious software.

Types of social engineering attacks
Pretexting



In these attacks, cyber criminals pretend they need certain information from their target in order to confirm the target's identity.

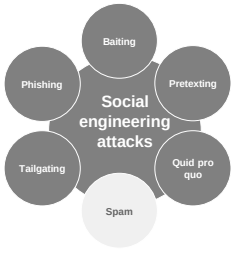
Types of social engineering attacks
Quid pro quo



In a quid pro quo attack, social engineers request information from an individual in exchange for something desirable.

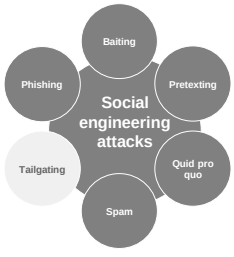
Types of social engineering attacks
Spam

Spam consists of bulk email messages sent to individuals without their permission. Spam emails can be malicious and expose you to malware infection or a loss of data.



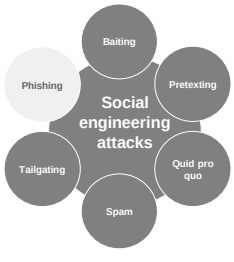
Types of social engineering attacks
Tailgating

Tailgating is when an unauthorized individual enters a secure location by following a person with legitimate access, without the employee's permission or knowledge.



Types of social engineering attacks
Phishing

Phishing is sending a fraudulent email, instant message or other web-based media to get someone to divulge any information.



Phishing is the most common type of social engineering attack used today. Most phishing emails seek to obtain information, include embedded hyperlinks or attached files, and often communicate threats, fear or a sense of urgency.

Passwords – as easy as 123456

The 25 worst passwords revealed

- If your password appears on this list, you should probably change it right away

1) **123456** (unchanged)
2) **password** (unchanged)
3) **12345678** (up 1)
4) **qwerty** (up 1)
5) **12345** (down 2)
6) **123456789** (unchanged)
7) **football** (up 3)
8) **1234** (down 1)
9) **1234567** (up 2)
10) **baseball** (down 2)
11) **welcome** (new)
12) **234567890** (new)
13) **abc123** (up 1)
14) **111111** (up 1)
15) **1qaz2wsx** (new)
16) **dragon** (down 7)
17) **master** (up 2)
18) **monkey** (down 6)
19) **letmein** (down 6)
20) **login** (new)
21) **princess** (new)
22) **qwertyuiop** (new)
23) **solo** (new)
24) **passw0rd** (new)
25) **starwars** (new)

The password is the basic factor in authentication

Weak passwords	Strong passwords
▸ **Four-digit year:** 19XX, 20XX	▸ Minimum password length of 8–12 characters
▸ **"Password":** pass, password, p@$$word	▸ A combination of upper- and lowercase letters, numbers and special characters.
▸ **Dictionary words:** "football," "baseball," "secure"	▸ Different from any of the last passwords used
▸ **Names:** name of your pet, parents, children	▸ Try to use different passwords for different services
▸ **Personal Information:** your name, email address, birthday	▸ **Use a passphrase instead of a password**
▸ **Keyboard patterns and sequences:** qwerty, asdf, 123456, abc123	

Create strong passwords

One way to create a secure password is to start with a word you will remember → e.g.,**"pamphlet"**

Add numbers, special characters and capitalization → Hence, you may come up with **"pAMPh$3let"**

Use a passphrase

- A passphrase is a phrase or series of words that is used to create a unique password. A passphrase is typically longer than passwords for additional security.

How to create a passphrase

- Create a phrase that is long and meaningful
- The phrase may be personal to you, so you can remember it easily
- Use the first character of each word to form a password or the entire phrase

Passphrase example

My **p**arents **b**ought **m**e **a** **c**ar **a**s **a** **g**raduation **g**ift **i**n **2**013.

Mpbmacaaggi2

I **w**as **h**ired **a**t **M**om **a**nd **M**om **o**n **J**une **1**8, **2**015.

IwhaMaMoJ12

Passwords

- **Use different passwords for every site**
  - Otherwise, one site getting hacked exposes all of your accounts
- **Use a *secure* password manager**
  - Creates a complex password for every site for you
  - You need to remember only one master pass phrase
  - Can be a vault for other important information

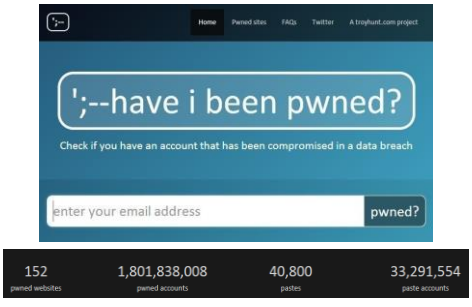
Two-factor authentication

- **What is it?**
  - Requires multiple things to gain access to an account:
    - Something you know
    - Something you have
- **Why is it good?**
  - Prevents someone who has your password from accessing an account
  - Notifies you when someone tries to access your account

Two-step authentication using Google Authenticator

- Provides a second factor of authentication to access your Google account
- If your username and password are ever compromised, the attacker will also need the PIN code to access your account
- Google Authenticator can be used for many personal sites too!

Watch for breaches in the news



https://haveibeenpwned.com

Typical privacy-type questions

Our data never changes

- Email address
- Phone number
- Education history
- Employment history
- Home address
- Date of birth
- City and state of birth
- Pet names
- Family names
- Favorite color
- Car
- School mascot
- Favorite sports teams
- Favorite movies
- Mother's maiden name
- Spouse's name
- Names of friends
- Address

- Use your password manager to make up answers to security questions and record them

Real-life phishing examples

We know to ignore these

Nice to Know You

Naomi Surugaba [azlin@moa.gov.my] Actions

Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli.
Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you're reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent's and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent's. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

But what about this one?

Fwd: Consulting Expense

Print all

hide details print original 13:54

from:
to:
date: 2017 Jan 13 13:54:20
subject: Consulting Expense
system labels: Inbox, Opened
user labels:

Barbara,

I will be sending you details shortly for a professional service expense that needs to go out. Can we process a wire payment for this expense today?

Thanks,

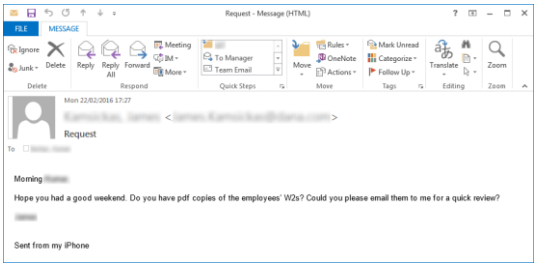
Larry

If you think people will not fall for this, they do

- The Federal Bureau of Investigation (FBI) has been keeping a running tally of the financial devastation visited on companies via CEO fraud scams.
- In June 2016, the FBI estimated that crooks had stolen nearly **$3.1b** from more than **22,000 victims** of these wire fraud schemes.

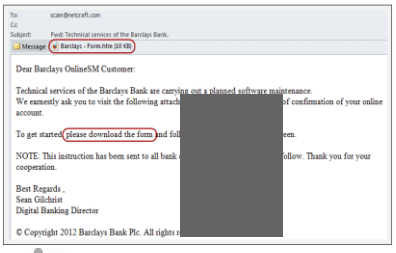
Source: https://krebsonsecurity.com/2017/02/irs-scam-blends-ceo-fraud-w-2-phishing/

Why would I need to email the W2 for employees?



We have seen lots of these over the past two months

Attachment phishing



To: scam@netcraft.com
Cc:
Subject: Fwd: Technical services of the Barclays Bank.
Message: Barclays - Form.htm (93 KB)

Dear Barclays OnlineSM Customer:

Technical services of the Barclays Bank are carrying out a planned software maintenance.
We earnestly ask you to visit the following attach[redacted]f confirmation of your online account.

To get started please download the form and foll[redacted]een.

NOTE: This instruction has been sent to all bank [redacted]ollow. Thank you for your cooperation.

Best Regards ,
Sean Gilchrist
Digital Banking Director

© Copyright 2012 Barclays Bank Plc. All rights r[redacted]

Do not open attachments in emails that you did not expect to receive.

Source: http://news.netcraft.com/archives/2012/11/13/phishing-attacks-using-html-attachments.html

Hover over the link

verizon

IMPORTANT ACCOUNT INFORMATION FROM VERIZON WIRELESS.

Update Your Profile Information

It has came to our attention that your payment method is out of date. Please update your payment method as soon as possible.

To update your profile, click: Sign in to My Verizon account and proceed with the update process.

http://ag.my/wp-admin/js/.sc/index.html

www.verizonwireless.com

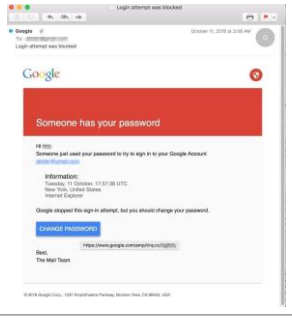
Thank you for using My Verizon.

Verizon. America's Largest 4G LTE Network. Learn More

© 2013 Verizon Wireless

Source: http://technews.olemiss.edu/files/2014/03/verizon-phishing.gif

Is this real?



Google

Someone has your password

Hi [redacted]
Someone just used your password to try to sign in to your Google Account [redacted]

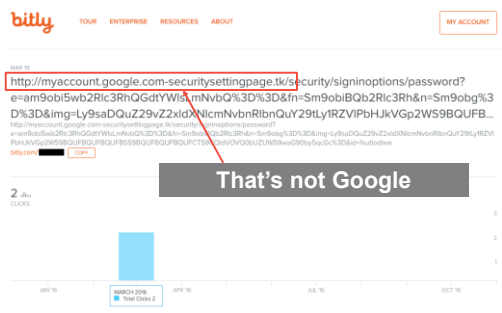
Information:
Tuesday, 11 October, 17:57:38 UTC
New York, United States
Internet Explorer

Google stopped this sign-in attempt, but you should change your password.

CHANGE PASSWORD

Best,
The Mail Team

What's wrong with this site?



Phishing can also occur via text messaging

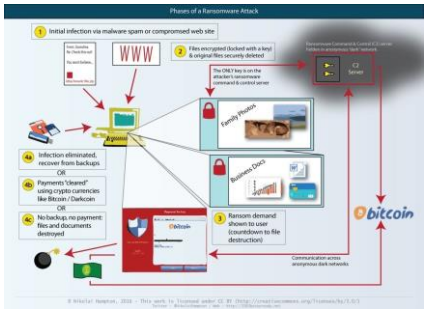
The Apple ID associated with this number is due to be terminated. To prevent this please confirm your details at http://supportatapple.com/ - Apple Inc.

Important Security Alert about your PayPal account.Please click the link bellow to read it: http://mobile-paypal.com[redacted].com

Texts/emails you should always avoid

- Any communication that you did not initiate
- Communications from your bank with links
- Communications from the IRS
- Communications from your credit card company with a call to action
- Unsolicited communication from your doctor, lawyer, accountant or other professional services person
- Random communication from your mortgage company
- Scary texts from a lender
- Promotion from your favorite game

Ransomware



What is social media?

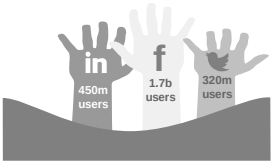
Social media are interactive platforms that allow people to create and share information over the internet. These platforms include web applications, websites and mobile apps.

Examples include:

Facebook	Pinterest	Discussion boards
Twitter	Google+	Blogs and wikis
Instagram	Snapchat	Any website "share" function that allows users to send content to their contacts
LinkedIn	Tumbler	
YouTube		

Social media sites are susceptible to privacy concerns

- Two of the most popular social media platforms are Facebook and Twitter.
- LinkedIn is the largest professional networking site.
- One million websites have integrated with Facebook.
- 25% of users don't bother with privacy settings.



IoT devices

IoT scanner

http://iotscanner.bullguard.com/

Tips to avoid social engineering

- Be skeptical of unusual or unexpected communications
- Be cautious in what you post online
- Be careful when opening attachments
- Speak up if something doesn't look right
- Lock your laptop screen: **do not** leave equipment unattended in public places
- Do not send personal or highly restricted information over the Internet without double-checking the validity of the website's URL (https:///...)

Tips

Migrate to modern operating systems and hardware platforms

The latest version of any operating system (OS) usually updates security features from the previous versions. Many of these security features are enabled by default and help prevent common attack vectors.

Install a comprehensive security suite

Install a comprehensive security suite that provides layered defense via anti-virus, anti-phishing, safe browsing, host-based intrusion prevention and firewall capabilities.

Install ad blockers for your web browsers.

Tips

Implement WPA2 on your wireless network

To keep your wireless communication confidential, ensure your wireless access point is using Wireless Protected Access 2 (WPA2) connection at home.

Implement strong passwords on all network devices

In addition to using a strong and complex password on your wireless access point, use a strong password on any network device that can be managed via web interface, including routers, printers and cameras.

Buyer beware

- **Beware of public things**
  - Public kiosk computer
  - Public Wi-Fi
  - Hotel computers

Questions?