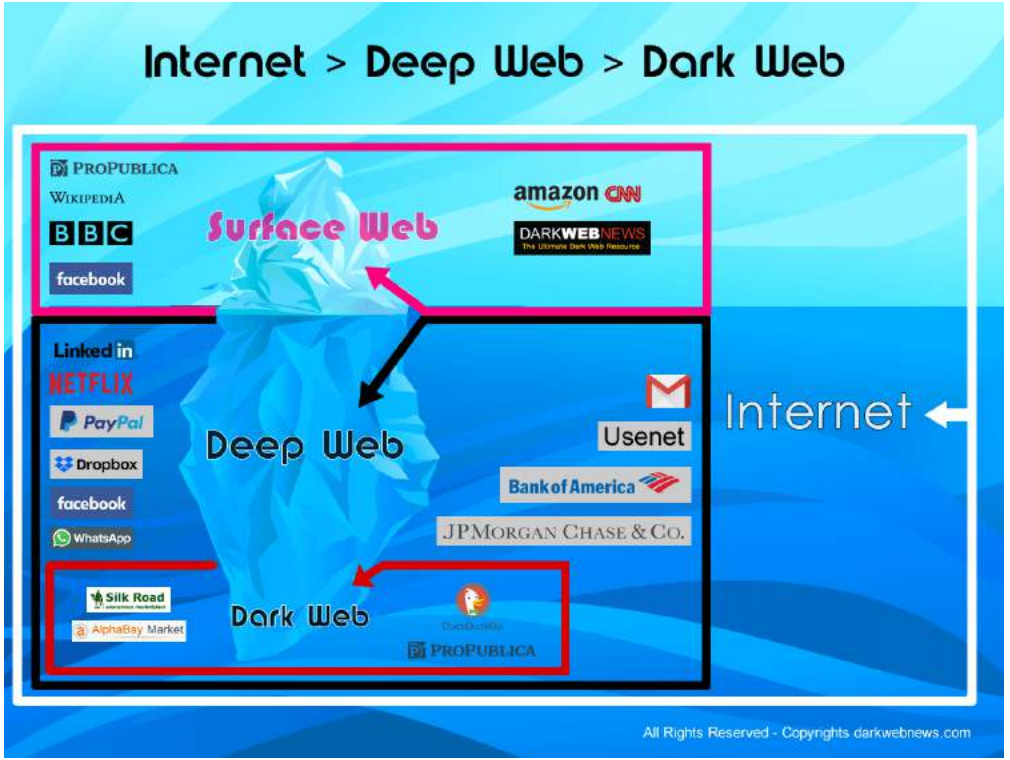
Digital Security

Avenidas January 26, 2018



Disclaimer

The Avenidas, Generations Lab class on CyberSecurity is provided as a public service, for informational purposes only. All information from this class or from the Generations Lab is presented without any representation, guaranty, or warranty whatsoever regarding the accuracy, relevance, or completeness of the information. **The information contained in this class, from Avenidas or from the Generations Lab is provided only as general information, which may be incomplete or outdated.** Please note that users of the Information are responsible for independently verifying any and all information and is responsible for use of any products included in the class. The inclusion of links from this class does not imply endorsement or support of any of the mentioned services, products, or providers.

Agenda

- The Cloud Overview
- Common Threats Defined
- Devices and Applications
- Passwords
- Browsers
- The Do’s and Don’t

Brief Overview on The Cloud

Question

- Who Here Uses the Cloud?
- Name some Apps that you use in the Cloud?

Think of the Cloud as an Office Building

Building Responsibilities

- Electricity
- Heating & Cooling
- Plumbing
- Parking
- Internet Connectivity
- Telephones
- Structural

Tenants may provide

- Products & Services Delivered to Consumers

The Cloud – Quick Overview

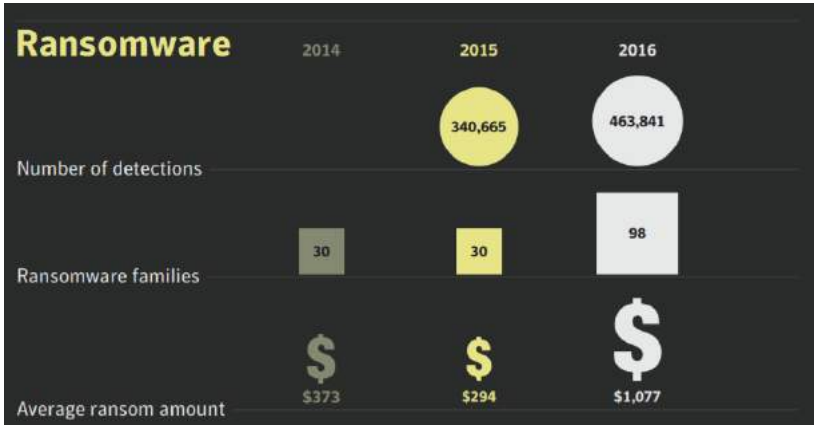
Before the Cloud (on Premise)	The Cloud
Programs and Applications bought and reside on home computer.	Applications reside on many managed servers. Centrally managed.
Need to buy license (separate) for all software, by OS, by Device.	Not required to buy license, sometimes can choose features. Pay Subscription
Need to maintain hardware and software upgrades or Pay for new versions.	Download a light application (interface) to access the services.

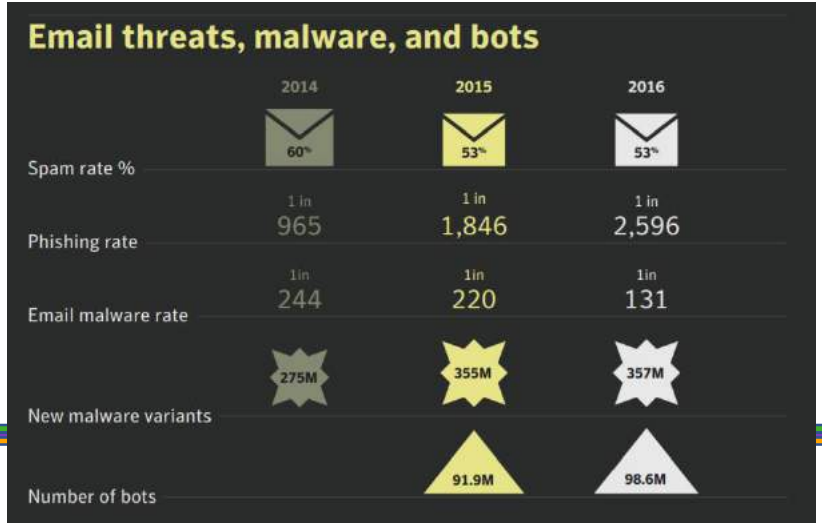
Cyber Security Overview - Threats

Online/Digital Security Threats

Security is a Process, Not a Product – Bruce Schneier

- 1 out of 3 people have received a Security Threat
- 2017 Ransomware attacks have doubled since Last Year
- 41% of Americans have experienced a fraudulent bank/bank card charge.





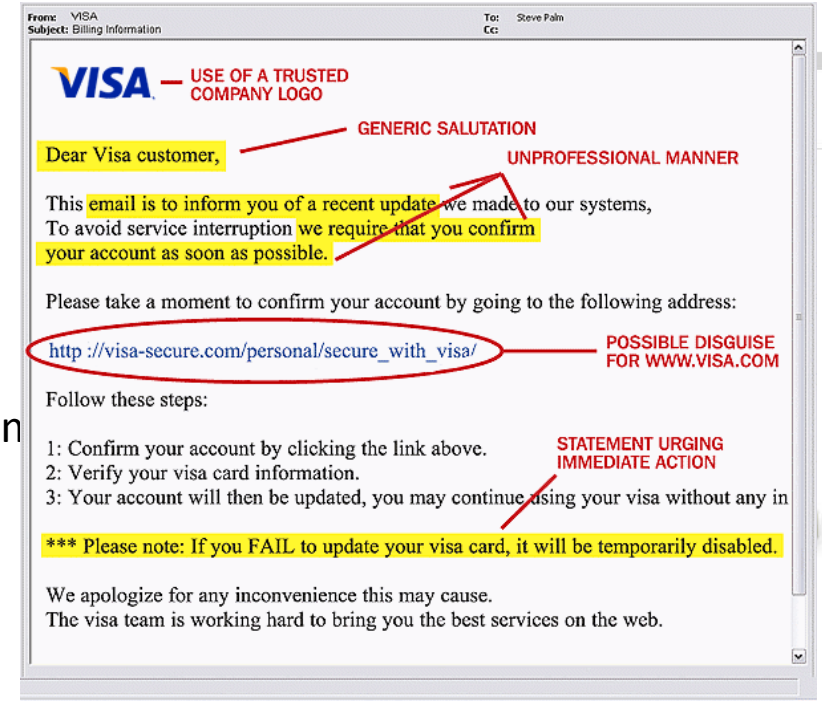
Scams by Type 2016

Definitions

- **PHISHING** - the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
- **CATFISH** - someone who pretends to be someone they're not using Facebook or other **social media** to create false identities, particularly to pursue deceptive online romances.
- **SPOOF** - is the creation of **email** messages with a forged sender address.
- **DDOS/DOS** – Distributed Denial of Service - the intentional paralyzing of a computer network by flooding it with data sent simultaneously from many individual computers.
- **MALWARE** – any program or file that is harmful to a computer user.
  - Ransomware, for example, is designed to infect a user's system and encrypt the data.
  - Trojan (RAT) is a malicious program that secretly creates a backdoor into an infected system.
  - Adware, infects computers with unwanted ads and degrading performance of the device or system
- **BOTS** can be used for either good or malicious intent. A malicious **bot** is self-propagating **malware** designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "botnet."

How can we Tell?

- SPOOF/PHISHING: think of as Fishing for information through mass emails.
  - Reputable Companies will NEVER have Spelling or Grammatical Errors.
  - Companies you do business with will Personalize.
  - Hover over the FROM: email address and check if it comes from the company
  - Hover over any link and see if the URL is from the company.
  - Rarely will ask to login from an email.
  - Reputable companies Don't Threaten.
  - If you don't do business with the company, don't call them.



Let's Practice

From: securservices@comcast.net
To:
Sent: 2018-01-12 7:05:29 AM
Subject: We noticed unusual activity in your PayPal account

PayPal

Dear Customer:

You recently changed or attempted to change your password, If you changed your password you can now log in to your PayPal or If you didn't change it, seems your account has been compromised.

What do I need to do?

Click here to login to your PayPal account and complete the steps required to secure your account. For your protection, account access will remain limited until you complete these steps.

The security of your PayPal account is a top priority for us and we want to work with you to protect it.

* * *These updates will take effect on September 1 th 2017. If you do not agree to the new User Agreement or the Debit Card Agreements, you may close your PayPal account or cancel your PayPal Debit Card before September 1 th, 2017.

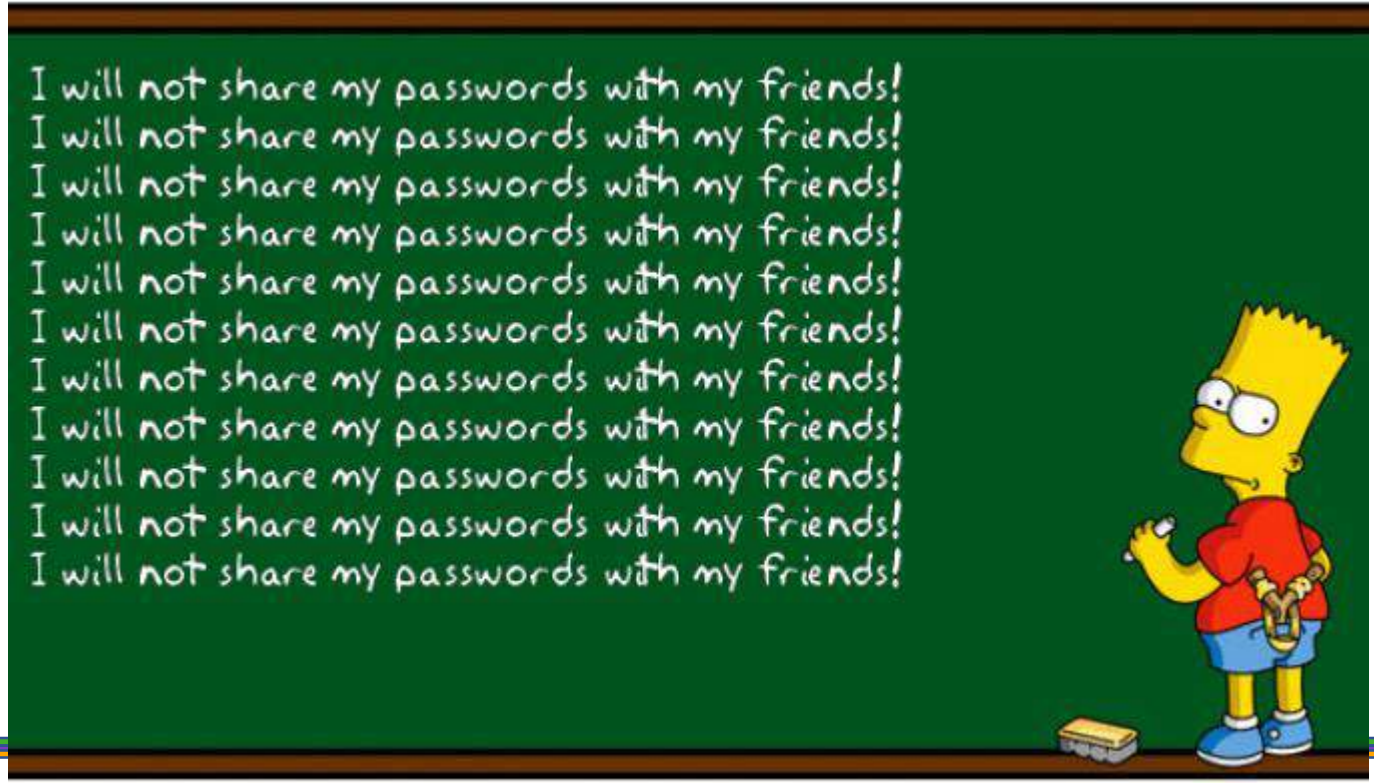
Thank you for being a PayPal customer.

Sincerely,
PayPal

Visa Service Department

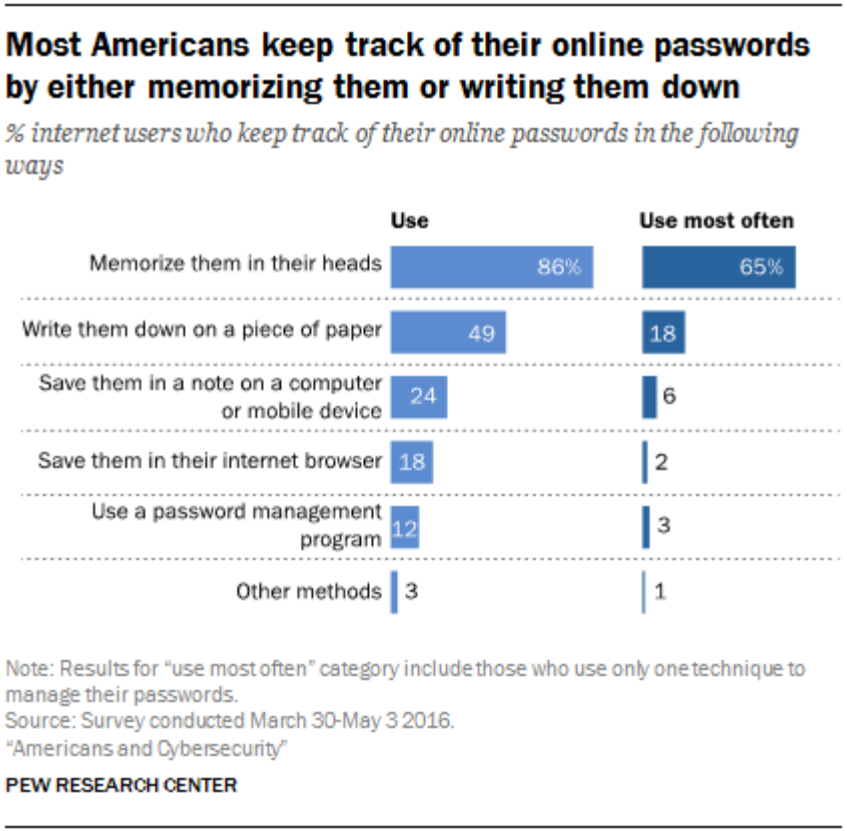
7/26/12 Thu,

Passwords


I will not share my passwords with my friends!
I will not share my passwords with my friends!
I will not share my passwords with my friends!
I will not share my passwords with my friends!
I will not share my passwords with my friends!
I will not share my passwords with my friends!
I will not share my passwords with my friends!
I will not share my passwords with my friends!
I will not share my passwords with my friends!
I will not share my passwords with my friends!
I will not share my passwords with my friends!

Passwords

- Passwords Are on the Front Line of Protection
- Do You?
  - Memorize?
  - Write them Down on Paper?
  - Store them on a device?
  - Use a Password Management System?



Passwords – A Matter of Math

Bill Burr's (former Manager of the National Institute of Standards and Technology) 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—***he regrets the error!***

Common Words

9806 possible words		Average time to crack based on number of guesses per second				
Size	**Possible combinations**	**1 trillion (expected future capability)**	**100 billion (large distributed system)**	**1 billion (distributed system or supercomputer)**	**100 million (small distributed system)**	**1 million (single computer)**
2	96.2 million	instant	instant	instant	instant	48 seconds
3	943 billion	instant	5 seconds	8 minutes	1 hour	5 days
4	9.25 quadrillion	8 minutes	13 hours	2 months	1 year	1 century
5	90.7 quintillion	2 months	14 years	14 centuries	144 centuries	-
6	889 sextillion	14 centuries	-	-	-	-
7	8.72 octillion	-	-	-	-	-

New National Institute of Standards and Technology were published in June. They recommend a random phrase of at least four words that make no sense together.

Password Comparisons

https://passwordcreator.org/commonwords.html - randomly generates passwords

Random Password Generator

Random	Writable	Shiftless	Fake Word	Common Words
⟶ ldG#.>qx*"#v	⟶ Fct3Kirt3Zwjzg	⟶ d43x[ ]68t;bg\	⟶ maursisseniurvexaptiorly	⟶ dirt concave boon grim sulk sown
⟶ `R;es1'/Z__;	⟶ KtWWhGX733rKGe	⟶ io'v.e,kxh;7zv	⟶ tourtaigrassustidnemierm	⟶ stack burnt doctor colon pour knelt
⟶ &QuV#)gm_4AM	⟶ nKGALgxnFbBmgz	⟶ O-ipag;a5e624`	⟶ deistokirgickeparfate	⟶ crimes unpaid gadget insider ceded masks
⟶ F\)Iot_}t?MR	⟶ 9M8h9jKYGr9QZX	⟶ u7,=.l//i\3-/l	⟶ glonolfescecaunseemiuy	⟶ axioms sturdy joked tread upkeep update
⟶ y~!h W4`,#&\	⟶ B7ptYkMyF63e7b	⟶ nokc7bv56[bb[e	⟶ doucceestrorgisraeffoxygelds	⟶ deft colder twists pistols bottom saves
⟶ ^fLo&4_</>)?	⟶ GqFj6rKQHBZL5p	⟶ j79xe 4`4j l5x	⟶ ventiompightethnireaspharts	⟶ dram gloat south sewn methods randy
⟶ oMOvfX`k*9E,	⟶ XmQRar7dRq4mQB	⟶ [w43`4'v1czfyi	⟶ goalfwarmfustatcheplosella	⟶ sustain stopped shining ace gives rented
⟶ ?W@'*/LsNv2,	⟶ c3FqkqT9Gt6FKP	⟶ O`/qn1dxcr/,6,	⟶ tucajommembryonceacieds	⟶ sonic sour dated ablaze papal mars
⟶ UN;#B*iB~qXs	⟶ zBc2Jt3bZWiRba	⟶ 9'uq'\b,-4qgq`	⟶ scrictingelmengitsensuille	⟶ kicked bowls scan motions scripts cola
⟶ G%x~g",Ah`3e	⟶ D37qx7XgDQp4tJ	⟶ 4m]o9ujtjn\t-'	⟶ yieldithemoaxindoptiof	⟶ froze ethics thine overs gel fig
Out of 540 sextillion possibilities	Out of 610 sextillion possibilities	Out of 345 sextillion possibilities	Out of 109 sextillion possibilities	Out of 889 sextillion possibilities

To Crack

Billion - Instant
Trillion - Seconds
Quadrillion - Minutes
Quintillion - Days/months
Sextillion - Years
Septillion - Centuries
Octillion - ?

Passwords

- Use a Password Keeper
- Find a system easy to remember
- Longer is better
- Store passwords in a safe place (I like to code them)
- If the system allows spaces, use them, increases complexity
- Avoid using words publicly known (current address, kids, pets…)

D0g_umbrella+P1ngP0ng
(dog umbrella ping pong)

*$e7enal1ig@t0r5inmyb^th
(seven alligators in my bath)

Devices and Browsers

BROWSER

Computers/OS

Safest Computers for Web Browsing

- ChromeBook – limited to run just Chrome OS and Google Apps. Low on Premise Storage. Small Attack Surface – very limited exposure to random Malware attacks.
- Mac OS – General purpose machine, sees fewer attacks due to smaller market share. However, Apple Demographic may be subject of targeted attacks.
- Windows – Dominant Market Share, designed to run any application. Need to work at securing device.
- Linux – Smaller eco-system but all open source, less Malware being designed to attack linux but need expertise to fully secure.

Browsers – Ever Changing Landscape

Popular Browsers

- Google Chrome – large extension eco-system to enhance security: choose Ad Blocker, Blur – integrated across devices
- Firefox – fell behind but catching up. Large extension eco-system doesn't auto integrate. Works w/legacy apps
- Opera: works well with older computers, some built in security functions like ad blocker.
- Safari: built in anti-phishing and pop-up blocker but weaker on SSL/TLS/encryption
- Internet Explorer – Most vulnerable; Microsoft Edge is MSFT's new version of a secure browser

Specialty Browsers

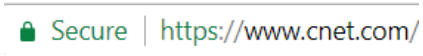
- Epic – strips out potentially vulnerable components. Prioritizes SSL connections
- Comodo Dragon/Ice Dragon – Chrome/Firefox derivatives. Can use Comodo's secure DNS servers.
- TOR – designed to be a privacy browser, not a security browser. Try's to anonymize user. Built to go through a separate infrastructure traveling through "hidden" relay servers.
- Dooble – Chrome based, disables insecure interfaces such as Flash and Java Script. Only allows HTTPS connections.

What's the Difference?

- HTTP: Unsecured Connection. Do NOT transmit Personal Information or conduct Transactions.
- HTTPS: Secured Connection, OK to conduct Personal Information Business or Transactions

Browser Technology Definitions

- Browser Security consists of two major topics
  - Security – protection against accessing device
  - Privacy – Primarily concerned with tracking – cookies, Browsing history, web cache…
  - DNS - Domain Name Server – resolves request to correct website
  - HTTP – Hypertext Transfer Protocol – translation from browser to internet
  - HTTPS – Secure Hypertext Transfer Protocol – Secure translation from browser to internet
  - Cookies – pieces of information that tracks activity
  - Flash (Adobe) – Animation/video software – known for vulnerabilities, slowly being replaced by HTML 5.
  - Java Script – Programming Language typically used for distributed content (web content, IoT programming, Android Development…)
  - Two Factor Authentication - referred to as two-step or multi-factor verification, is a security process in which the user provides two authentication factors to verify they are who they say they are.



Computer/Browser Review

- Some Computers and Browsers are more secure than others
  - Some recommend using a dedicated device for sensitive online work
  - Not all browsers are the same. Extensions enhance security and privacy
    - Blur: Free password keeper and masks passwords, credit card transactions, randomizes site passwords.
    - LastPass: Free password keeper
    - Ad Blocker and Ad Blocker Plus – stops pop up ads
    - HTTPS Everywhere
  - Search on “Best <insert browser> Extensions Security”

Do’s and Don’ts for Online Security

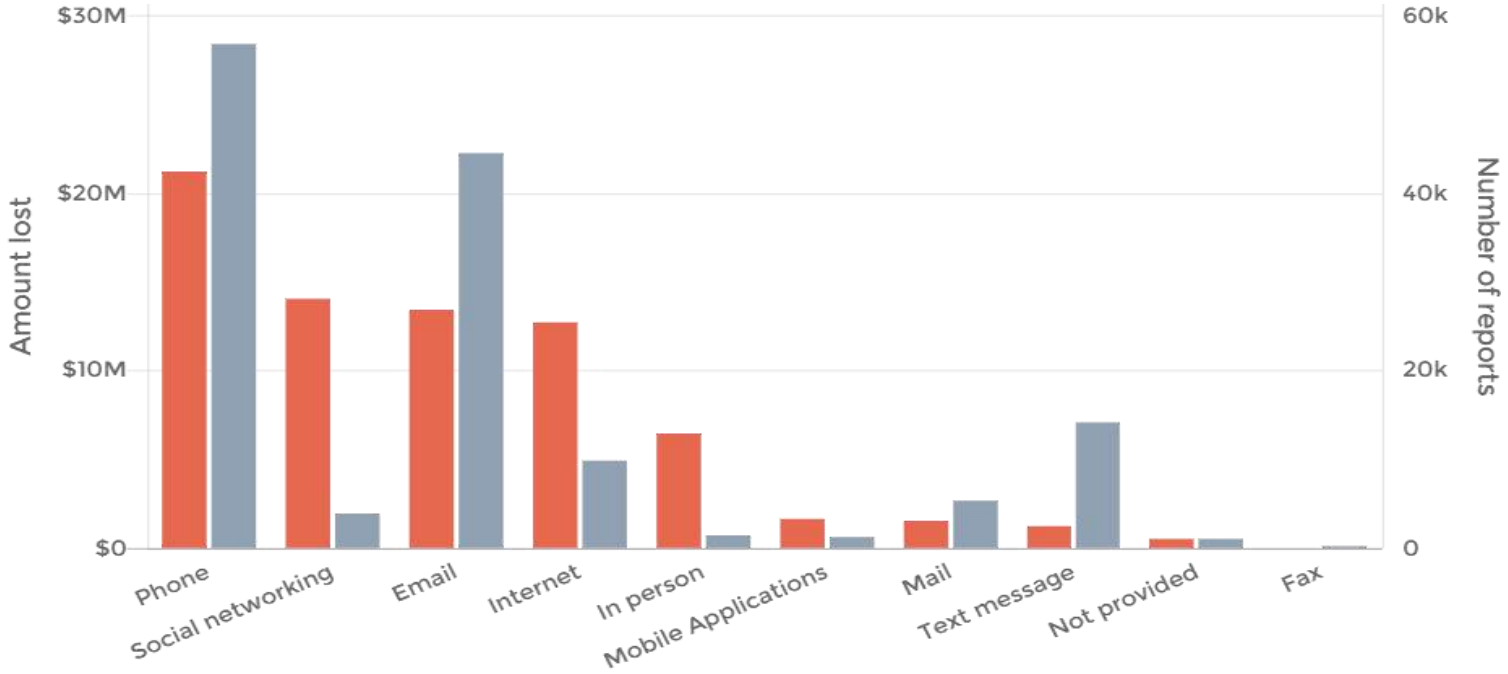
- DON’T Click on Links in email unless from a Trusted Friend AND it makes sense.
- DON’T Give out personal information such as Social Security Number, Full Birthdate, Home Address…..
- DON’T conduct secure business on an Unprotected/Public Computer
- DON’T use a link from an email
- DON’T download attachments from unknown people (PDF’s and JPG or generally safer NEVER open .EXE’s).
- DON’T Click on Pop Up ads

Do's and Don'ts for Online Security

- DO password protect cell phones, tablets, computers
- DO take advantage of multi-factor authentication
- DO make a strong password, change frequently
- DO update system and applications
- DO backup information in a secure cloud location or external hard drive.
- DO look for the HTTPS or lock sign in your browser address list
- DO Download application from trusted sites (Apple App store, Google Play Store, Amazon Store…).

Questions

Scams By Delivery Method



resources

- https://www.nytimes.com/2016/11/17/technology/personaltech/encryption-privacy.html
- https://www.digitaltrends.com/computing/best-browser-internet-explorer-vs-chrome-vs-firefox-vs-safari-vs-edge/
- https://www.techworld.com/security/best-8-secure-browsers-3246550/
- https://en.softonic.com/download/comodo-dragon/windows/redirect-post-download
- https://www.usatoday.com/story/tech/columnist/komando/2016/01/15/3-biggest-security-threats-2016/78839018/
- https://www.computerworld.com/article/3163627/linux/if-you-want-privacy-you-need-to-run-linux.html
- http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/
- https://lifehacker.com/5796816/why-multiword-phrases-make-more-secure-passwords-than-incomprehensible-gibberish
- https://www.lifewire.com/creating-a-strong-password-system-153307

What is The Cloud (computing)

- Data Center Serving General Needs
  - Storage, Applications, Infrastructure
- Manage Common Components– Operating Systems, Performance Tuning, Upgrades
- Able to be used on different devices.
- Typically Subscription fees – pay as you go, pay what you need.
- Common Terms
  - PAAS – Platform as a Service – provides managed Environment for developers
  - SAAS – Software as a Service – provides applications, centrally managed.