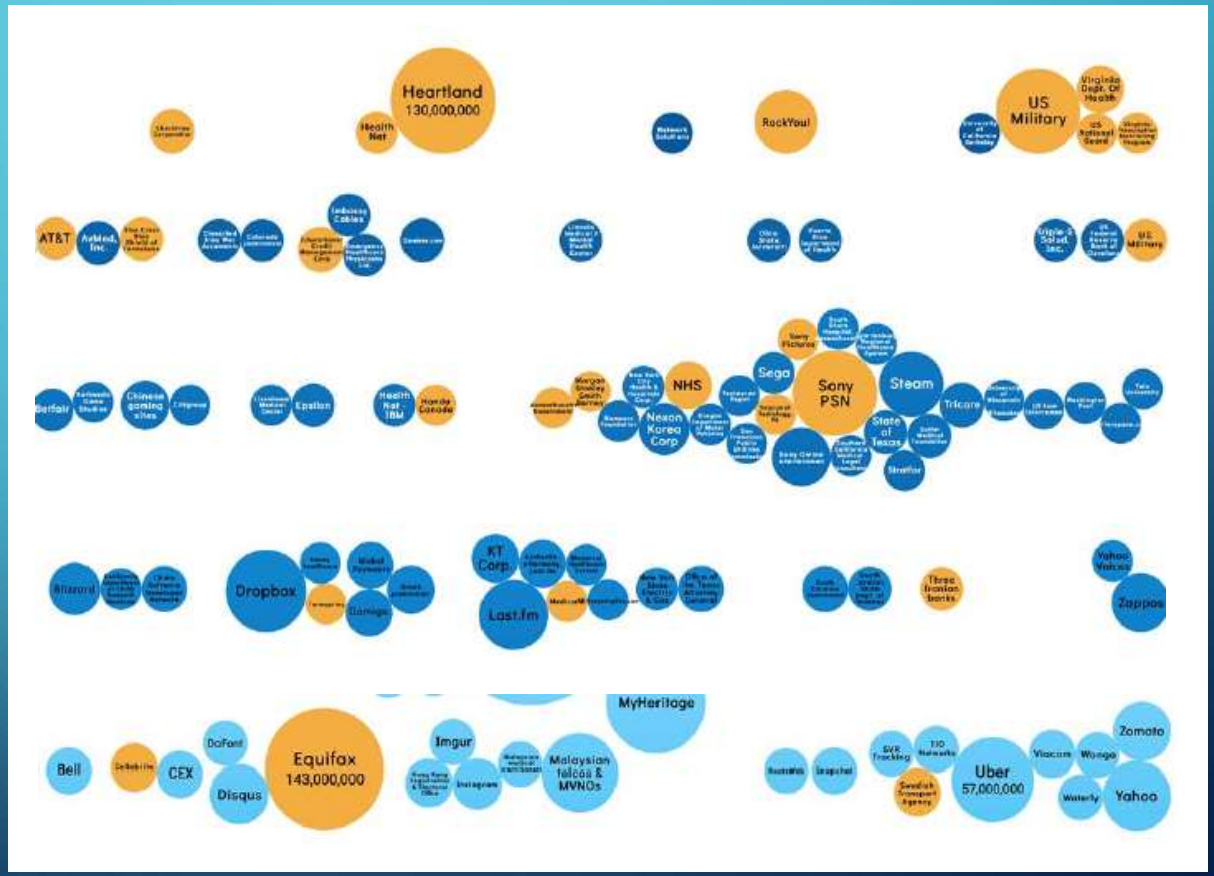
CORPORATE CUSTOMER TRAINING

CYBERSECURITY AND CUSTOMER ACCOUNT TAKE OVER (CATO)

First American Bank and Trust
A Banking Tradition Since 1910

DATA BREACH

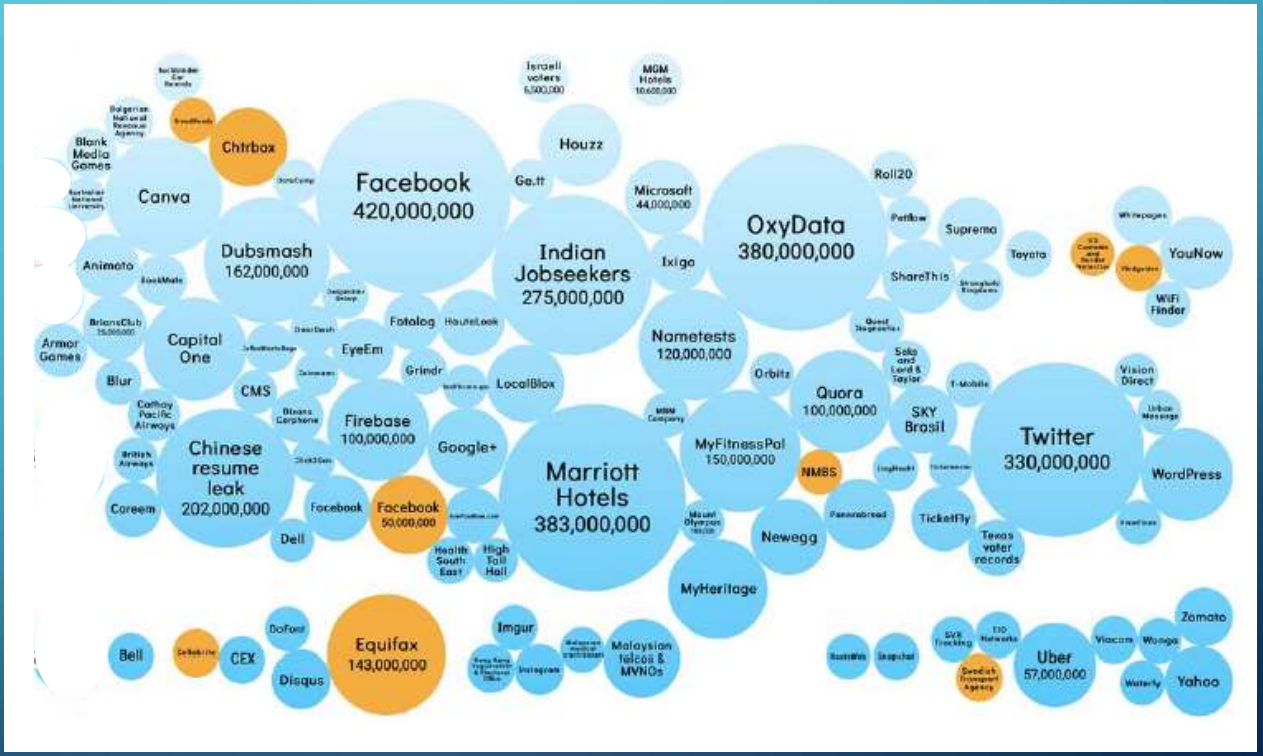
A GROWING PROBLEM …



DATA BREACH

A GROWING PROBLEM

TODAY



2020 DATA BREACHES

JANUARY 2020

INCIDENT: Customer support database unprotected

- 280 million customer records
  - ✓ Emails, IP addresses, support case details
  - ✓ No other personal information compromised

FEBRUARY 2020

INCIDENT: Former employee responsible for breach

- "Undisclosed number of customers"
  - ✓Name, SSN, drivers license info, address, DOB, account numbers, etc.

FEBRUARY 2020

INCIDENT: Third-party vendor theft

- Employee laptop theft
  - ✓654k members personal and medical info expose

FEBRUARY 2020

INCIDENT: 10.6 million customer records published to hacking forum

- Personal info and contact details for tourists, travelers, celebrities, CEOs, government officials, etc.
  - ✓ Security incident uncovered in summer 2019

MARCH 2020

INCIDENT: Employee and customer information accessed

- Compromised employee email
  - ✓Names, addresses, SSN
  - ✓Passport and drivers license numbers
  - ✓Credit card and account information

MARCH 2020

INCIDENT: Employee email account compromised - Third-party email vendor

- Unknown amount of personal information
  - ✓Name, addresses, SSN
  - ✓Drivers license numbers, billing information

MARCH 2020

INCIDENT: Third-party application breach

- 5.2 million guest records impacted
  - ✓Names, emails, phone numbers
  - ✓Linked loyalty programs
  - ✓2nd known breach in 2 years

OBJECTIVES OF THE CRIMINAL

- Access or manipulate the stolen data
- Destruction of the stolen data
- Extortion or ransom for recovery of the stolen data
- Disruption of business operations

- the fraudulent practice of sending emails purporting to be from reputable companies, or management, in order to induce individuals or install malware in order to reveal personal information, such as passwords and credit card numbers.

PHISHING OBJECTIVES

- Install malware
- Steal credentials
- Obtain information
- Perform a task

PHISHING STATISTICS

…FROM THE 2019 VERIZON DATA BREACH INVESTIGATION REPORT

- 3% of users will click on any phishing campaign
- Average 16 minutes until the first click on a phishing campaign
- First report from a savvy user will arrive after an average of 28 minutes

EXAMPLE

From: Susan Fry [mailto:sfry@yourcompany.com]
Sent: Tuesday, January 9, 2018 9:25 AM
To: Hamil, James <james.hamil@yourcompany.com.
Subject: Please handle ASAP

– External email. Forward any suspicious emails to bad@yourcompany.com –

Attached Phishing Email

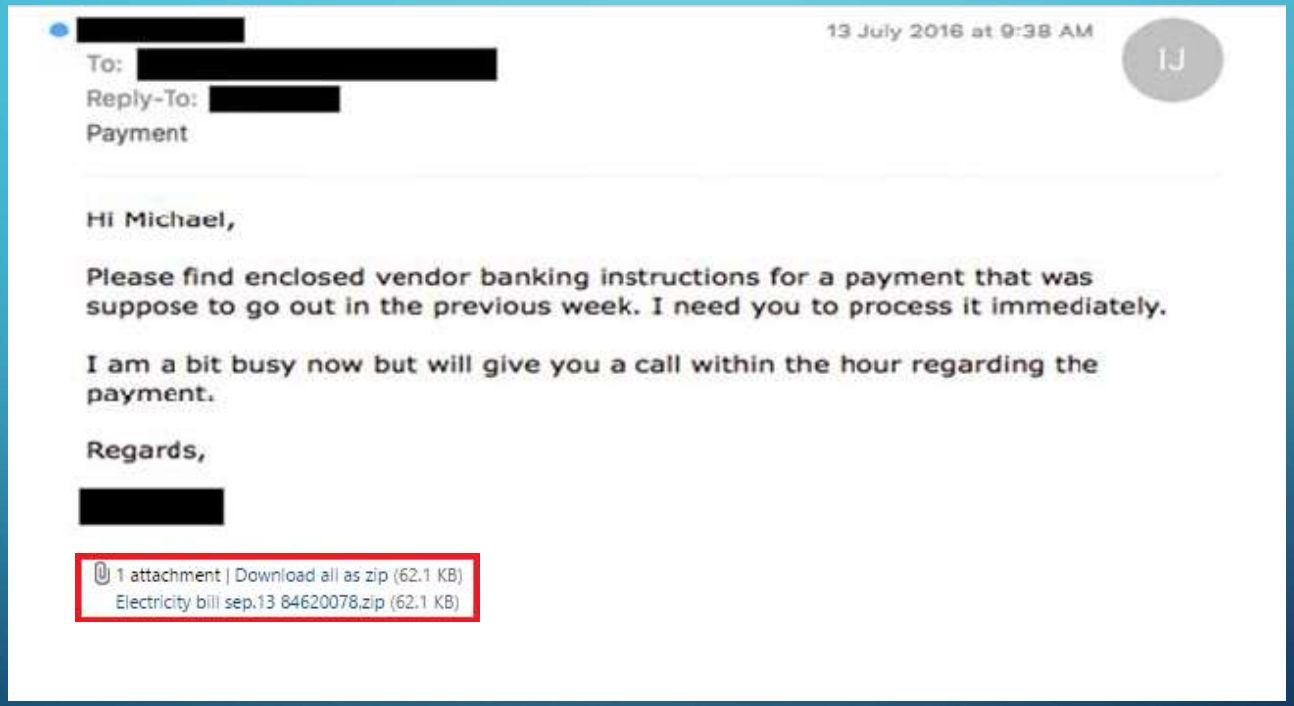
Hi James,

I'm currently tied up in a meeting for the next six hours, but we have a vendor saying we're late on paying an invoice. Can you handle the attached ASAP? I can't take calls, so just email me if you have questions.

Susan Fry
Chief Operating Officer
sfry@yourcompany.com

Sent from my iPhone, please excuse typos

EXAMPLE



[redacted]

13 July 2016 at 9:38 AM

IJ

To: [redacted]

Reply-To: [redacted]

Payment

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

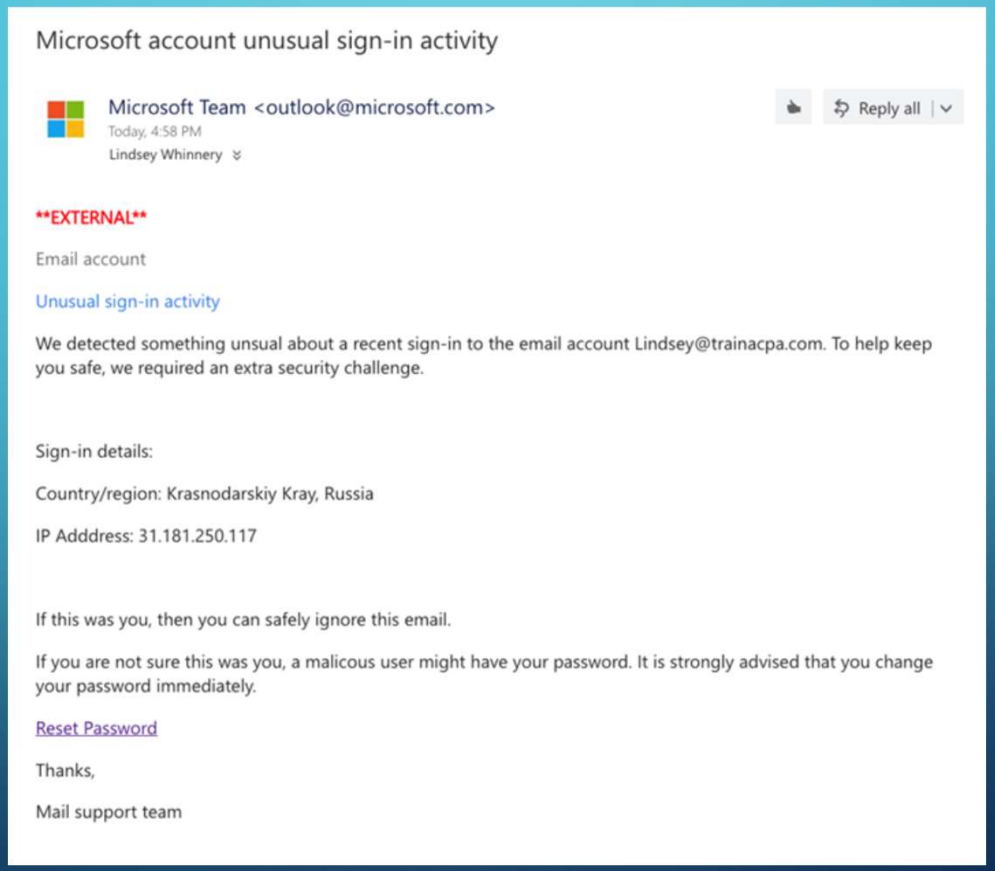
I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

1 attachment | Download all as zip (62.1 KB)
Electricity bill sep.13 84620078.zip (62.1 KB)

EXAMPLE



Microsoft account unusual sign-in activity

Microsoft Team <outlook@microsoft.com>
Today, 4:58 PM
Lindsey Whinnery

Reply all

EXTERNAL

Email account

Unusual sign-in activity

We detected something unusual about a recent sign-in to the email account Lindsey@trainacpa.com. To help keep you safe, we required an extra security challenge.

Sign-in details:

Country/region: Krasnodarskiy Kray, Russia

IP Adddress: 31.181.250.117

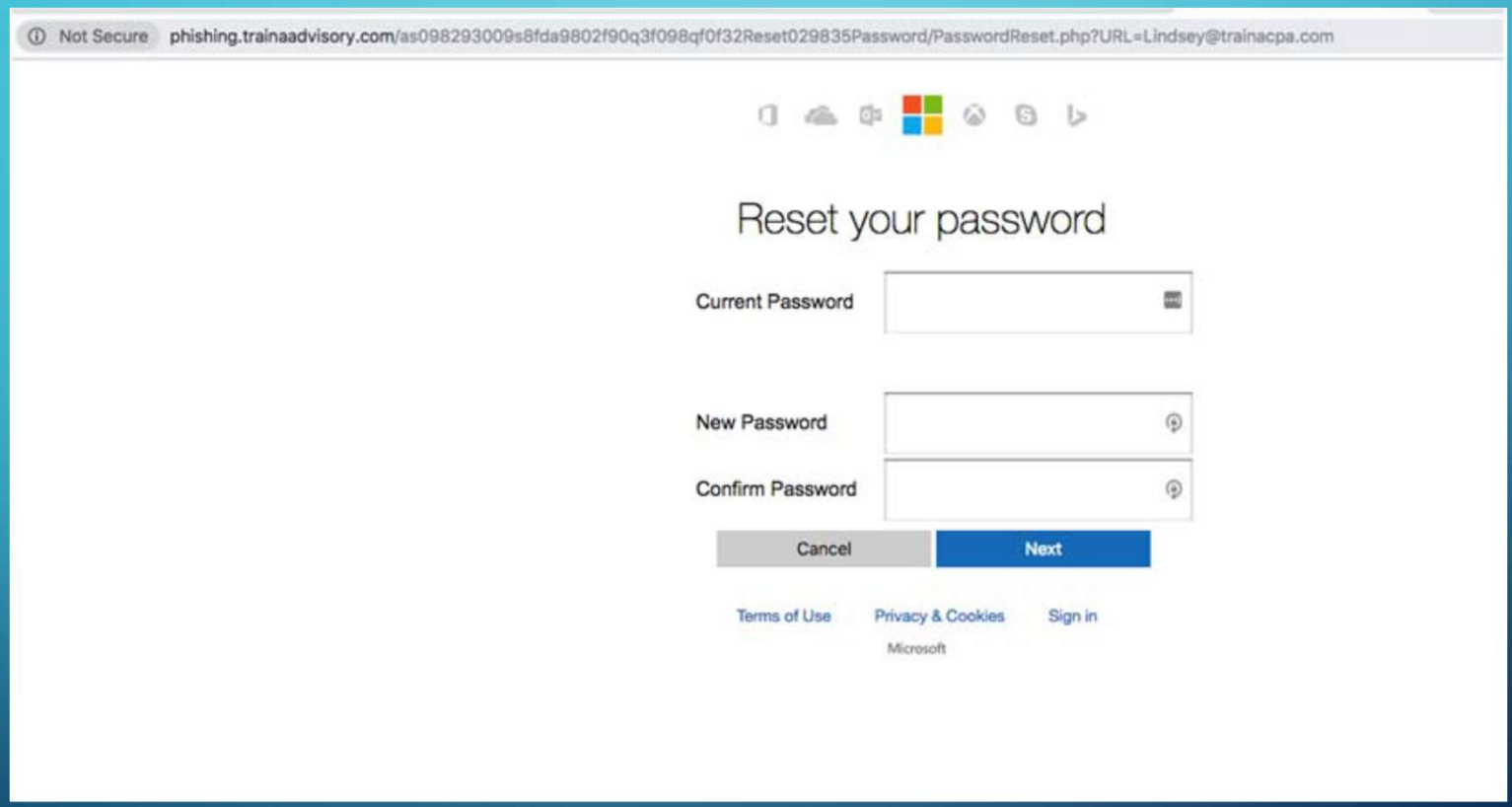
If this was you, then you can safely ignore this email.

If you are not sure this was you, a malicous user might have your password. It is strongly advised that you change your password immediately.

Reset Password

Thanks,

Mail support team


Not Secure
phishing.trainaadvisory.com/as098293009s8fda9802f90q3f098qf0f32Reset029835Password/PasswordReset.php?URL=Lindsey@trainacpa.com
Reset your password
Current Password
New Password
Confirm Password
Cancel
Next
Terms of Use
Privacy & Cookies
Sign in
Microsoft

ONE CLICK… THAT'S ALL IT TAKES!

RANSOMWARE DEFINITION

- **Ransomware** is a form of ***malware*** that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.
- Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

HOW RANSOMWARE WORKS

- There are a number of vectors ransomware can take to access a computer. One of the most common delivery systems is phishing spam — attachments that come to the victim in an email, masquerading as a file they should trust. Once they're downloaded and opened, they can take over the victim's computer.
- The user is presented with a message explaining that their files are now are now inaccessible and will only be decrypted if the victim sends an untraceable Bitcoin payment to the attacker.


Wanna Decryptor 1.0
Ooops, your files have been encrypted!
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files for free. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
How Do I Pay?
Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28
Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
QR Code
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1
Copy
Check Payment
Decrypt

HOW TO PREVENT RANSOMWARE

- Keep your **operating system patched and up-to-date** to ensure you have fewer vulnerabilities to exploit.
- Don't **install software or give it administrative privileges** unless you know exactly what it is and what it does.
- Install **antivirus software,** which detects malicious programs like ransomware as they arrive, and **whitelisting software,** which prevents unauthorized applications from executing in the first place.
- And, of course, **back up your files,** frequently and automatically! That won't stop a malware attack, but it can make the damage caused by one much less significant.

CORPORATE ACCOUNT TAKEOVER (CATO)

Corporate Account Takeover is a form of business identity theft where cyber thieves gain control of a business' bank account by stealing employee passwords and other valid credentials. Thieves can then initiate fraudulent wire and ACH transactions to accounts controlled by the thieves.

CORPORATE ACCOUNT TAKEOVER (CATO)

- Criminals gain access to bank account after obtaining user credentials through:
  - Phishing emails
  - Keylogger malwares

CATO DAMAGES

- Add new user accounts
- Initiate unauthorized external transfers
- Hijack transmitted ACH payroll files and change recipients.
- Request outgoing Wires
- Steal funds using other external transfer options (Bill Pay, P2P, etc.)
- Access to confidential data for additional attacks

CATO PROTECTION & PREVENTION

Controls Established by the Bank

- **Multi-factor authentication** - a security feature that verifies a user's identity by requiring multiple credentials
- **New user alerts** – texts or emails send each time a new user is created.
- **Device authentication/restriction -** the process of identifying and verifying the identity of a system or person in a secure manner. For example, if you log on to a device with a username and password, you are being authenticated as the device is checking that you are really who you say you are.
- **Enhanced high risk transaction controls –** monitoring of hardware and access history to determine unauthorized patterns of logins and request in order to discover and verify transaction legitimacy with the user.

CATO PROTECTION & PREVENTION

Controls to be Establish by the Customer

- **Understand Phishing**
- **Anti-Malware Management –** maintain update malware protection software.
- **Follow Bank's recommended Security Procedures**
- **Maintain Patch Management –** the process that helps acquire, test and install multiple **patches** (code changes) on existing applications and software tools on a computer, enabling systems to stay updated on existing security patches and determining which patches are the appropriate ones.
- **Protect Wi-Fi Networks –** maintain stringent wi-fi keys and restrict outside user access
- **Avoid Public Wi-Fi**
- **Maintain Adequate Passwords**

PASSWORD SECURITY

TOP 20 MOST COMMON PASSWORDS

(as a percentage of all passwords)

1.	123456	4.1%	11.	login	0.2%
2.	password	1.3%	12.	welcome	0.2%
3.	12345	0.8%	13.	loveme	0.2%
4.	1234	0.6%	14.	hottie	0.2%
5.	football	0.3%	15.	abc123	0.2%
6.	qwerty	0.3%	16.	121212	0.2%
7.	1234567890	0.3%	17.	123654789	0.2%
8.	1234567	0.3%	18.	flower	0.2%
9.	princess	0.3%	19.	passw0rd	0.2%
10.	solo	0.2%	20.	dragon	0.1%

PASSWORD SECURITY

- Numbers, characters, symbols should be mixed
- Avoid common words
- >12 characters, if possible
- Unique and private passwords, don't share
- Business vs personal, use different for each

WEB SURFING PRECAUTIONS

- Avoid questionable websites (https:)
- Cautious downloads (Follow anti-malware software warnings)
- Current browser (Keep updated)
- Inspect URL (Verify legitimacy)
- Malvertising (Don't click on pop-up ads)

DATA STORAGE

- Save files to appropriate location
- Beware
  - External drives
  - Mobile devices
  - Rogue cloud storage and sharing

VENDOR MANAGEMENT

- Analyze all New vendor relationships
  - Maintain procedures for evaluating new vendors
  - Conduct a risk assessment before establishing a relationship
  - Contract review should include cybersecurity
  - Approval procedures should be outlined to include proper reviews
- Existing vendor relationships
  - Periodic oversight procedures should address an annual review.

TRAINING FOR YOUR EMPLOYEES

- Training methods vary
  - ✓Seminar, emails, newsletters
- Anyone can teach!
- Training should be completed
  - ✓Upon hire
  - ✓Annually
  - ✓Continuously