

The background of the slide features a dark blue field with a complex network of glowing blue circles and lines, resembling a molecular or digital structure. In the center, a white shield icon with a cross inside is positioned above a hand that is reaching up towards it. A black rectangular banner is placed over the middle of the image, containing the title text in white.

IT SECURITY TRAINING FOR BRYCON EMPLOYEES

October 2017

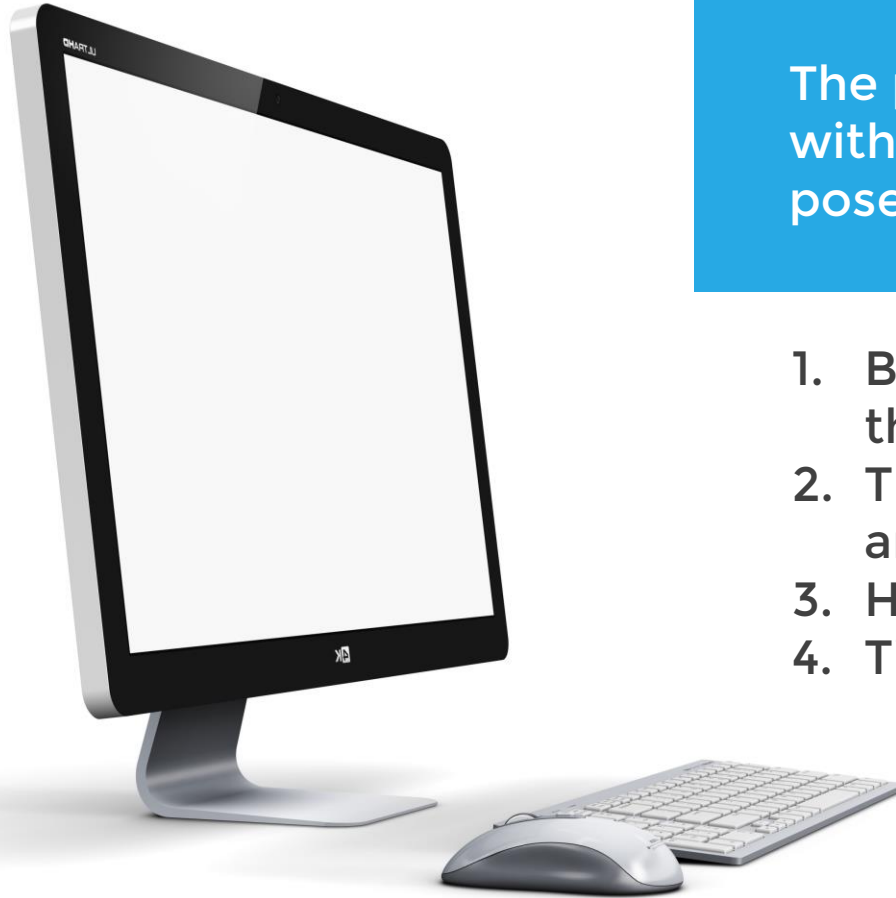
2375 E. Camelback Rd, Suite #600,
Phoenix, Arizona 85016

www.clearviewit.com

Call us today: 866-326-7214



TRAINING GOALS



The purpose of this training is to provide Brycon employees with an overview of the IT security landscape, the threats posed to Brycon and its employees, and:

1. Basic understanding of the threat landscape including the evolution of threats and deterrence
2. The dangers of a breach to Brycon and its employees and business partners
3. How to create strong passwords
4. Tips for combatting attacks aimed at users

DICTIONARY OF TERMS



Attack Surface

Attack Vector - A shortcut in the shape of a square or rectangle that goes on the start menu. Some Live Tiles are live and display dynamic data (such as the weather).

Botnet - One of these. They normally denote either a menu or an expansion of a menu.

Malware - This is how you browse the file system and is represented by this icon.

Ransomware - The actual act of verifying login credentials.

Active Directory/Windows domain - A network of Windows devices and servers that share a single authentication database.

Cloud - Someone else's computer.

Cache - A locally stored copy of something that lives someplace else (like images on frequently visited websites).

Desktop

Laptop

Workstation

Mobile Device Tablet

PC

Box

Computer

Tower

Convertible

Station

CURRENT THREAT LANDSCAPE

The Telegraph

Hackers leak more Game of Thrones scripts and HBO emails in demand for millions in ransom money



Global Ransomware Attack Stuns Systems in Up to 74 Countries

Businesses and hospitals were disrupted in a massive wave of cyberattacks Friday. Such attacks have increased by more than 500 percent in recent years.



Another big malware attack ripples across the world

The New York Times

Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say

The New York Times

Yahoo Says 1 Billion User Accounts Were Hacked



Petya ransomware: Cyberattack costs could hit \$300m for shipping giant Maersk



OPM government data breach impacted 21.5 million

CURRENT THREAT LANDSCAPE



What do macOS and Android have in common? Both are booming malware markets

Healthcare IT News

San Antonio's largest OB-GYN provider breached by keylogger malware

Hackers spent one month on the servers of The Institute for Women's Health, stealing both financial and personal health data.

ars TECHNICA

Ransomware app hosted in Google Play infects unsuspecting Android user



St. Mark's Ransomware Attack Could Affect 33K Patients

Recent potential data breaches include two ransomware attacks, two phishing attacks, and a keylogger virus.



Hackers look to shut down factories for pay
Malware creates virus that sets up ransom situation



Nearly half of federal IT managers report breach in last six months: research

CURRENT THREAT LANDSCAPE



New malware and adware spreading through Facebook Messenger



How these fake Facebook and LinkedIn profiles tricked people into friending state-backed hackers



Hackers next target could be the US electric grid



White House advisory group warns of '9/11-level cyber attack'



**NotPetya aftermath:
Companies lost
hundreds of millions**



U.S. Warship Collisions Raise Cyberattack Fears

The background of the slide features a person wearing a dark hoodie, seen from the side, typing on a laptop. The laptop screen is glowing with a bright blue light. The background is a dark, textured surface with a grid of glowing blue binary code (0s and 1s) and various digital icons such as a mail envelope, a location pin, a car, a camera, and a Wi-Fi symbol. The overall theme is digital security and cyber threats.

WHO IS ATTACKING - ATTACKER PROFILES AND MOTIVATIONS

WHO IS ATTACKING - ATTACKER PROFILES AND MOTIVATIONS

Nation States and Terrorists

Industrial
Espionage

Influence
Opinion

Effect
Change

Revenue

Warfare



China says will tighten controls over intellectual property theft



'Strong Links' Now Tie North Korea To WannaCry Ransomware Pandemic



NORTH KOREA: HACKERS TARGETED U.S. MILITARY WORKERS VIA JOB AD SPAM DURING MISSILE TESTS



Experts Suspect Russia Is Using Ukraine As A Cyberwar Testing Ground

WHO IS ATTACKING - ATTACKER PROFILES AND MOTIVATIONS

Competitors and Corporate Insiders



The American Greed Report: Corporate spying costs billions, can it be stopped?



Dutch arrest man over suspected spying at Siemens

WHO IS ATTACKING - ATTACKER PROFILES AND MOTIVATIONS

Organized Crime



Revenue

FINANCIAL TIMES

Organised crime finally embraces cyber theft

BUSINESS INSIDER

Organized Crime Hackers Are The True Threat To American Infrastructure

CSO FROM IDG

Cybercrime: Much more organized

Cybercrime offers the potential for immense profits. So it is no surprise that the digital “mob” has moved into the space. According to some experts, there is no such thing as “disorganized cybercrime” any more

WHO IS ATTACKING - ATTACKER PROFILES AND MOTIVATIONS


Individuals



Revenue



Influence /
“Hactivism”



Personal
Gratification
(lulz)

The Telegraph

Hackers steal 2.5 million PlayStation and Xbox players' details in major breach

Forbes

PSN Down As Sony, Blizzard, Riot And Others Are Under Siege By Hackers [Update: SOE President's Plane Diverted By Bomb Scare]

PBS

Hacktivists launch more cyberattacks against local, state governments

U.S. News

Mossack Fonseca Blames Panama Papers Leak on Hackers

WHO IS ATTACKING - ATTACKER PROFILES AND MOTIVATIONS

Fellow Employees

Revenue

Revenge

Professional
Advancement

Unintentional
Disclosure

TECHSPOT

Former AMD, Intel engineer pleads guilty to stealing sensitive documents

MASS LIVE

Former Tufts Health Plan employee sentenced for stealing personal data of more than 8,700 customers

★ StarTribune

Thousands of students' personal info mistakenly e-mailed in S. Washington Co. data breach

Back-to-school e-mail in east metro errantly sent with private information.

The Register

US engineer in the clink for wrecking ex-bosses' smart meter radio masts with Pink Floyd lyrics



WHAT IS SENSITIVE DATA?

WHAT IS SENSITIVE DATA

BRYCON DATA



HR Data
W2s & other IRS Forms
Payroll Data
Employee Health Data



Internal Communications
(email, IM, phone calls,
schedules)



Partner/ Vendor/Client
Data, Intellectual
Property, and
Communications

What other
Brycon
Internal data
is
considered
sensitive?

WHAT IS SENSITIVE DATA

PERSONAL DATA



WHAT IS SENSITIVE DATA?



PHYSICAL CONTROL AND ACCESS:

Printers



Climate Control



Equipment



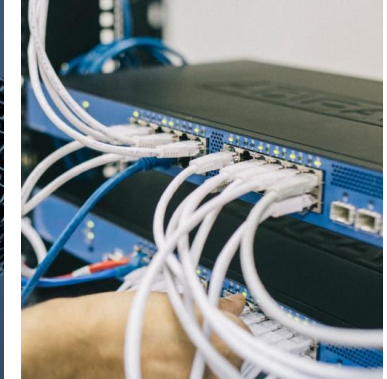
Webcams



Microphones



Denial of Service



WHAT IS BRYCON TRYING TO PROTECT? - RECAP



VULNERABILITIES, EXPLOITS, AND ATTACKS



The quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally.

What is Vulnerability?

A software tool designed to take advantage of a flaw in a computer system, typically for malicious purposes such as installing malware.

What is an Exploit?

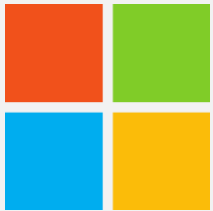
A vulnerability that is unknown to the vendor.

What is a Zero-Day Vulnerability?

VULNERABILITIES, EXPLOITS, AND ATTACKS



Microsoft
Windows



Microsoft
Office



Java, Flash
Player, Adobe
Acrobat



Browser, Add-
ins, Extensions

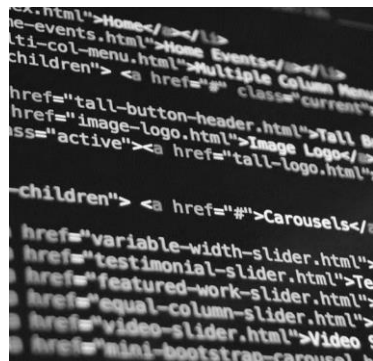


Network-
Connected
Device



VULNERABILITIES, EXPLOITS, AND ATTACKS

GOALS OF AN ATTACK:



Malicious
Code
Execution



Credential
Harvesting



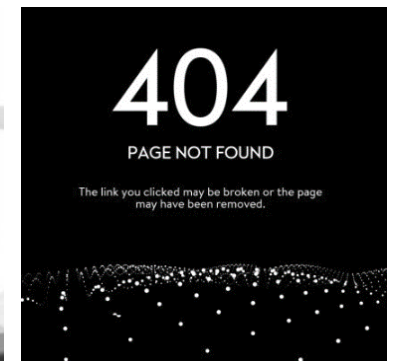
Payment



Control /
Manipulation



Data theft



Denial of
Service

VULNERABILITIES, EXPLOITS, AND ATTACKS



ATTACK VECTORS

Phishing
Spear Phishing Attack
Whaling Attack
Infected USB device



Social Engineering:

W2
Wire Transfers
Endangered family member
IRS/Microsoft



Android apps Internal
Employees
Lost/Stolen Device
(laptop/smartphone/tablet)



PROACTIVE SECURITY MEASURES



- Perimeter scanning, analysis, and filtering of Internet traffic (based on destination and payload)
- Windows end-point (Desktop PCs, laptops, Surface Pros) perform behavior-based malware scanning and DNS/IP-based network filtering
- Windows Server real-time signature-based virus scanning
- Email server antivirus/antimalware/antispam scanning and filtering as well as reputation-based sender checks
- Purchase/install the latest versions of Windows and Microsoft Office
- Automatically patch Windows, Microsoft Office, and major 3rd-party applications (e.g. Adobe Reader, Java, Flash, Chrome, etc.)
- Local Administrator rights are restricted (most groups)
- Windows Group Policies are customized to restrict the ability of malware to run
- Full server and data backups are performed automatically every day and stored offsite

WHAT ARE THE KEYS TO SECURITY?



Password



Patching (Updating)



Employee Training



WHAT MAKES A GOOD PASSWORD



Length
(Comic)

CHARACTERISTICS OF A BAD PASSWORD

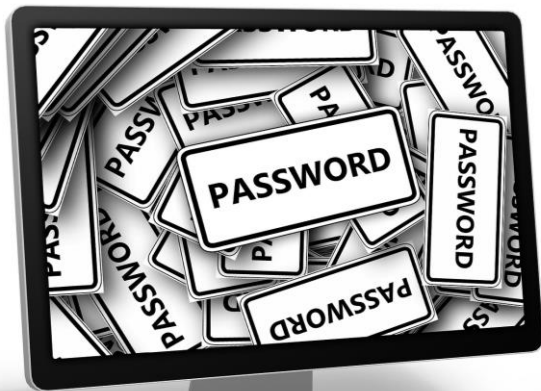
Contains any of the following (in any form):

- Brycon
- Construction
- User's name
- User's job title (including abbreviations)
- User's site name (e.g. FAB6, Ocotillo, Tesla, Intel, AZI, etc.)
- Physical location or building name

Utilizes an easily guessable sequence (e.g. qwertyuiop, 1q2w3e4r5t, 123qwe, zxcvbnm)

Utilizes any of the following passwords from the "Worst Passwords of 2016" list:

- | | |
|--------------|-------------|
| - 123456 | - abc123 |
| - password | - admin |
| - 12345 | - 121212 |
| - 12345678 | - flower |
| - football | - passw0rd |
| - qwerty | - dragon |
| - 1234567890 | - sunshine |
| - 1234567 | - master |
| - princess | - hottie |
| - 1234 | - loveme |
| - login | - zaq1zaq1 |
| - welcome | - password1 |
| - solo | |



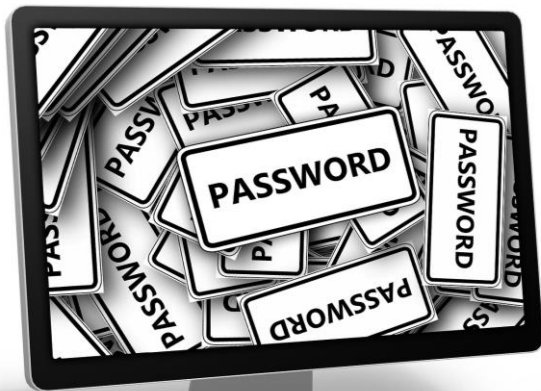
CHARACTERISTICS OF A BAD PASSWORD



Contains only a single word that can be found in a dictionary, including foreign language, or exists in slang, dialect, or jargon

Contains personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters

Contains common words spelled backward, or preceded or followed by a number (for example "Password1")



PASSWORD DOS AND DON'TS

DOS

- Confirm maximum length and allowed characters when creating a new password
- Use 2-Factor authentication when available
- Use a password manager (e.g. LastPass)
- Focus on length over complexity

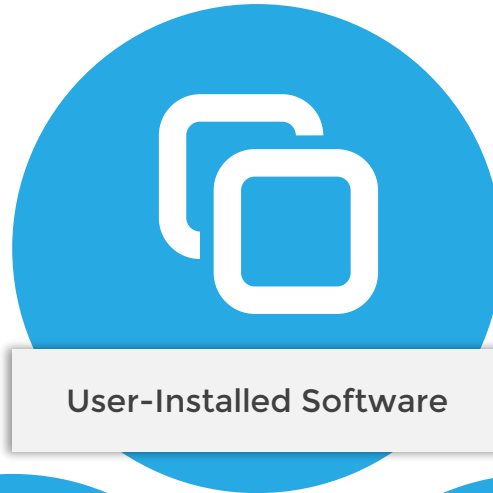
DON'TS

- Sync Passwords between sites or services
- Reuse passwords (even if a number is change such as "New user10" to "New user11")
- Share passwords with co-workers
- Use easy to guess/research answers to secret questions

PATCHING



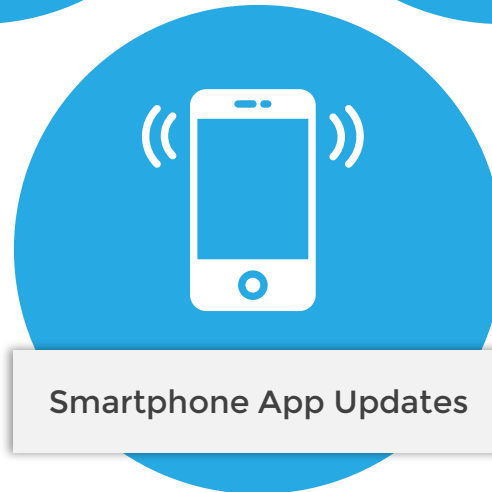
Browser Add-in



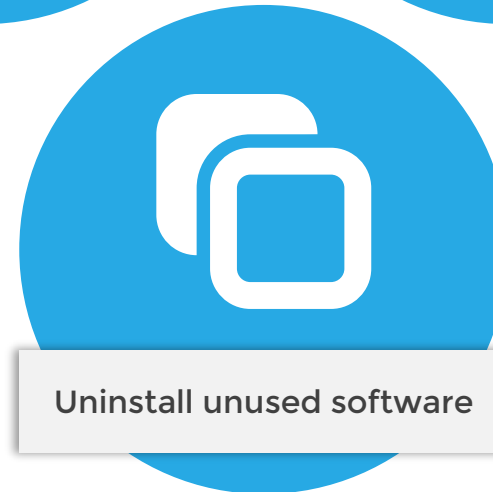
User-Installed Software



Android / iOS Updates



Smartphone App Updates



Uninstall unused software

EMPLOYEE TRAINING: BROWSING THE NET



Be very careful with what you click

Searching Google, Bing, and Yahoo

Exercise caution when clicking links, especially when searching high-risk topics (e.g. pop culture)

Social Media

Like-jacking: occurs when criminals post fake Facebook “like” buttons to webpages. Users who click the button don’t “like” the page, but instead download malware

Link-jacking: this is a practice used to redirect one website’s links to another which hackers use to redirect users from trusted websites to malware infected websites that hide drive-by downloads or other types of infections.

Website URL shortening services

bit.ly, goo.gl, tinyurl.com can mask malicious URLs

EMPLOYEE TRAINING: BROWSING THE NET



Be very careful with what you click

Using address bar
(versus searching)

HTTP versus HTTPS

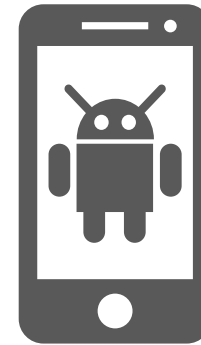
EMPLOYEE TRAINING: KEEPING YOUR MOBILE DEVICE SECURE



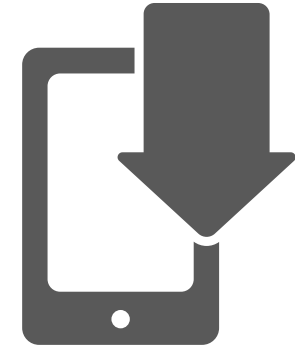
Set Screen locks on
Android/iOS devices



Immediately report
lost or stolen devices



Don't root your
phone



Only install software
from trusted sources

EMPLOYEE TRAINING: READING EMAIL



Junk Email

screenshot here

Email Properties

screenshot here

Macros

screenshot here

EMPLOYEE TRAINING: INSTALL MOBILE APPS



screenshots here

EMPLOYEE TRAINING: OTHER RECOMMENDATIONS



Cover unused webcams
with electrical tape



Avoid using USB storage
media



Avoid using open WiFi,
especially with non-HTTPS
sites

