Critical Mass: Resources

There are 13 items in the Resources section.

Classification Policy

Page from Gizmo's employee handbook detailing how data should be classified

- Public data can be made generally available without approval
- Private data's loss or unauthorized disclosure could impair or cause harm to the organization

Public:

- Board of Director Profiles
- Sales Presentations
- Mission Statement
- Product Guides

Private:

- Gizmo ID Badges
- Pictures of a Data Closet
- Quarterly Financials
- Customer Email Addresses

An addendum from October 2018 adds that Quarterly Financials are no longer Private and can be considered Public.

Critical Mass: Resources

Security Poster

10 security promises from Gizmo's security awareness team

1. I will follow security policies and procedures to the best of my ability!
2. I will not leave my devices unattended or unlocked!
3. I will feel no curiosity to open suspicious links or attachments in my inbox!
4. I will securely destroy sensitive data in the proper shred bins!
5. I will be aware of my surroundings!
6. I will not connect to unknown WiFi connections without a VPN!
7. I will enable multi-factor authentication (MFA) wherever possible!
8. I will never reuse passwords!
9. I will not plug unknown removable media devices into my computer!
10. I will avoid autofill and autosave features online!

Critical Mass: Resources

livingsecurity

Journal

Two notebook pages with hand-written phishing ideas

Phish Idea 1:

- Leverage the fear and awareness around the new internal Gizmo company
- Prey on the fear that it may affect ALL employees, and that they may not get overtime pay or travel allowances anymore
- Make the sender address look legit
- Attach a malicious PDF

Phish Idea 2:

- Impersonate DREW, the VP of Engineering, to target the HR department with a referral
- Try and get a backdoor on their systems
- Send over an engineering resume in a Word document (.docx) enabled with a macro
- Avoid any unusual urgency

Critical Mass: Resources

livingsecurity

Journal, continued

Phish Idea 3:

- Impersonate the Gizmo CEO, KYLE BAKER
- Get the Finance department to wire money, ASAP
- Target accounts payable
- Use a reference link that goes to a deposit page I setup: https://moneymefundzplz.com/customer0029478

Critical Mass: Resources

Notebook

A yellow legal pad with drawings and some brainstorming items

Random Writing:

- MASSIVE
- EAGLE EYE “K”

Phone Number:

- 585-404-3878

1st Target:

- Ask about kids
- Empathize
- Escalate for a report

2nd Target:

- Change identity
- Right to the point
- Get the second half of the secure passcode (the first half is “emerald”)

Critical Mass: Resources

Ongoing Investigation - Progress Report

An official report from Detective Mark Hernandez, detailing a review made March 2, 2020

- Perpetrator continues to elude the investigators but has been sending taunting emails
- Perpetrator was able to compromise a computer terminal belonging to an individual with privileged access
- Believed that the perpetrator plans to compromise an account used for payroll and flee with the stolen money
- Identity of the person whose computer was compromised is unknown, but they have black hair, they do not wear glasses, and they tend to wear a watch every day (they may also wear non-collared shirts to the office almost exclusively)
- Anonymous tip from Seattle turned out to be a dead end
- Interviews with Gizmo employees have been completed and testimony is being compiled for handoff to the district attorney
- Follow-up interviews with management and leadership will be next Wednesday
- Warrants are continuing to be served
- Working with Judge Smith and his clerk, Caitlin

Critical Mass: Resources

Camera Manual

Quickstart guide for Raptor Security Systems with sections:

- Getting started
- Recording and Playback
- Included in the Box
- Declaration of Conformity
- Connect to Computer
- Software Features
- View on System
- Camera Setup

- Default Credentials

Model	User	Password
Falcon Series - Model 3	admin	admin
Falcon Series - Model 5	manager	password
Falcon Series - Model 7	monitor	1234
Hawk Series - Model 1	sysadmin	PASSWORD
Hawk Series - Model 2	root	ADMIN
Hawk Series - Model 3	operator	Password
Eagle Eye Series - Pro D	admin1	pw123
Eagle Eye Series - Pro G	anonymous	1234admin
Eagle Eye Series - Pro K	superuser	abc123
Osprey Series - Model 2i2	user	sysadmin
Osprey Series - Model 2i4	camera	Admin

Critical Mass: Resources

livingsecurity

Paul

Name: Paul Richard Campbell
Occupation: Scrum Master
File number: 0284LZ

Sex: male
Hair color: brown
Eye color: brown
Height: 5’10”
Weight: 175
Country of origin: Canada

Favorite animal: narwhal
Family: no family connections

Critical Mass: Resources

livingsecurity

James

Name: James Harris
Occupation: Executive Director
File number: CFPR67

Sex: male
Hair color: black
Eye color: blue
Height: 6’2”
Weight: 195
Country of origin: USA

Favorite animal: narwhal
Family: cousin is Senator Reginald Harris

Critical Mass: Resources

livingsecurity

Emily

Name: Emily Sara Watson
Occupation: Technical Coordinator
File number: PQQR98

Sex: female
Hair color: black
Eye color: brown
Height: 5’7”
Weight: 130
Country of origin: Canada

Favorite animal: fox
Family: mother lives in Halifax, father deceased

Critical Mass: Resources

livingsecurity

Olivia

Name: Olivia Gray
Occupation: Technical Analyst
File number: 1786RT

Sex: female
Hair color: blonde/brown
Eye color: green
Height: 5’6”
Weight: 125
Country of origin: Canada

Favorite animal: narwhal
Family: divorced, no children

Critical Mass: Resources

livingsecurity

George

Name: George Thompson
Occupation: Vice President, Sales
File number: MBCR09

Sex: male
Hair color: black
Eye color: green
Height: 6’1”
Weight: 185
Country of origin: USA

Favorite animal: dog
Family: married, three kids, parents deceased

Critical Mass: Resources

livingsecurity

Kate

Name: Kate Lee
Occupation: Project Manager
File number: 8436DF

Sex: female
Hair color: black
Eye color: green
Height: 5’4”
Weight: 118
Country of origin: Canada

Favorite animal: fox
Family: married, one child

Critical Mass: Resources

livingsecurity

Blog Post

An article on the seven deadly sins of working from home, which include:

1. Untrusted WiFi (like your neighbor's WiFi)
2. VPN turned off (or not using a VPN)
3. Leaving computers unattended (including desktops)
4. Work data on personal devices (like TV screen-shares or casts)
5. Work data left out in open (on desks, tables, et cetera)
6. Leaving devices unlocked (phones, tablets, et cetera)
7. Leaving IoT devices unsecured (even doorbells and thermostats)

Critical Mass: Exercises

There are 8 exercises throughout the game:

1. In exercise 1, you are completing an arrest warrant by filling out the redacted boxes correctly. Review the employee case files in the Resources section to find the correct person and add their information.

2. In exercise 2, you are recreating three phishing emails described as business email compromise, or BEC. known as “vishing”, against Western Marketing. Use the Journal from the Resources section to see the ideas behind Olivia’s original email phishes.

3. In exercise 3, you are classifying the leaked information as either public or private. Refer to the Classification Policy from the Resources section to determine the correct classification for each item, then drag it into place in the puzzle.

4. In exercise 4, you are finding missing words in sentences about insider threats. Check out the Security Poster in the Resources section. Then, drag the right words into the correct slots to complete the exercise.

5. In exercise 5, you are inside Olivia’s apartment. You need to click on the security violations she committed. Review the Blog Post in the Resources section to know what to look out for.

Exercises, continued

6. In exercise 6, you need to crack a code Olivia made by inserting a missing phone number. Review the Notebook in the Resources section to find the information you need.

7. In exercise 7, you are retracing several voice phishing attack, known as “vishing”, to see what information Olivia got from her co-workers. Use the Notebook in the Resources section to follow her steps.

8. In exercise 8, you are signing into Raptor Security Systems, then selecting the co-worker whose device was compromised by Olivia. Refer to the Camera Manual and the Ongoing Investigation - Progress Report to finish the exercise.