Social Engineering

Austin Mercado, Joceyln Morales, Diana Maldonado Luberto, Annabel Mejia Cortes, Carmen Lopez

2023-04-22

Pretexting – Jocelyn Morales

Introduction

1. Pretexting is one of the different types of social engineering attacks. It is formulated by an attacker staging a situation that requires an individual to share their private information. An example of this could be a fraud call, where a fraudster pretends to be a governing figure or someone from a bank and begins reaching out to victims, who are then tricked into giving out their personal details. Majority of the times, this data is used in malicious ways.

Content

1. What are the most common dialogues/templates used when pretexting a victim?

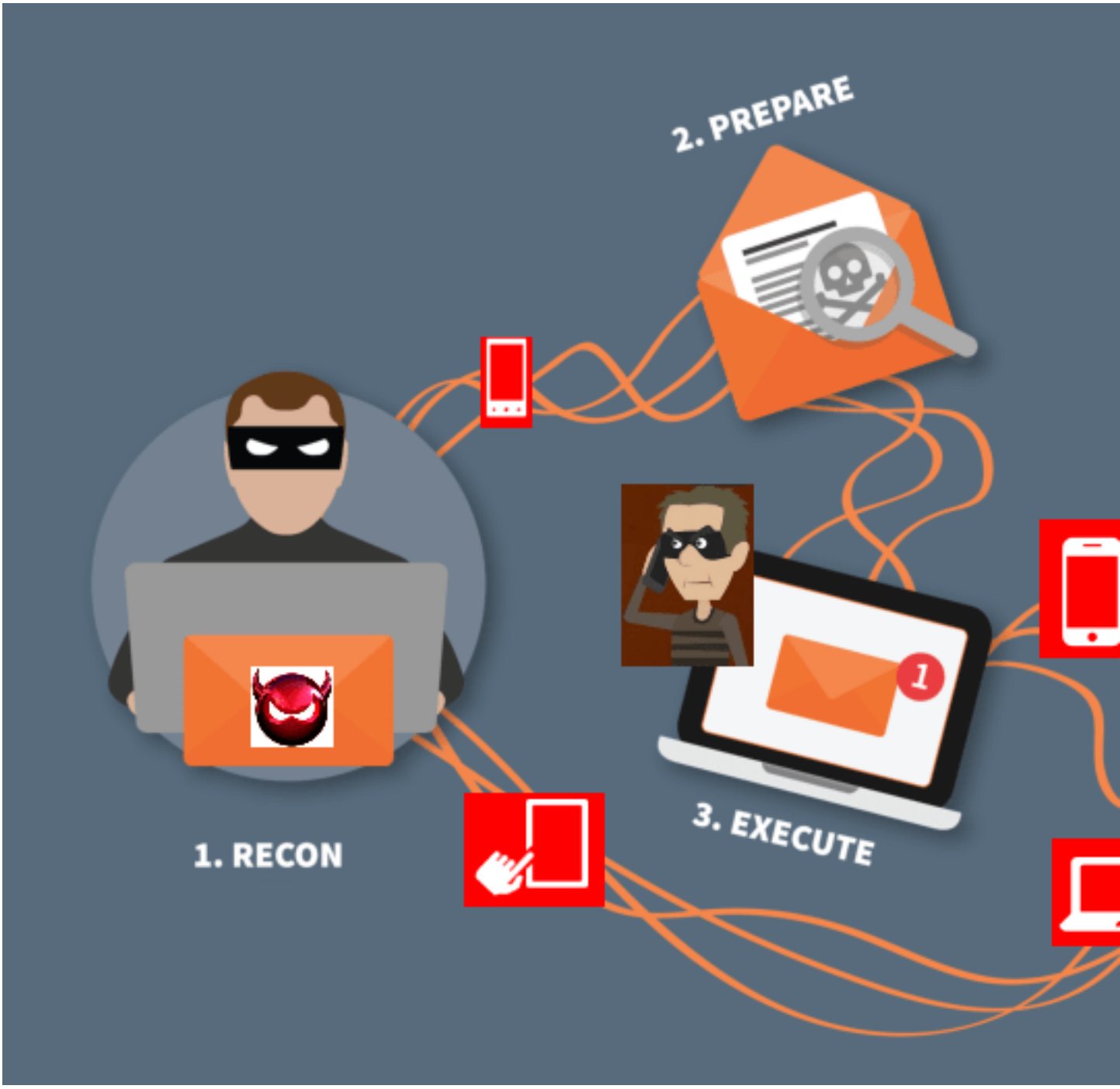
   The most common dialogue used when a hacker is attempting to pretext a victim, is by masking themselves as a bank that needs information from the user to verify a transaction. Where the victim sends their personal data, and the hacker extorts that.

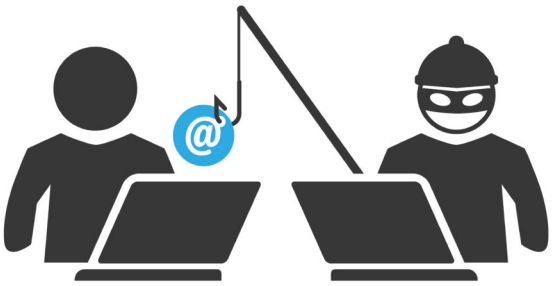
2. How to notice when a message or call is malignant.

   To identify a malignant call, look for signs of command repetitions if the caller keeps using the same words and attempting to gain some sort of information, you should hang up.

3. How are targets chosen.

   Targets are chosen when they have access to certain data the hacker needs or wants. At times individuals can be chosen at random when a perpetrator comes across their phone number.


2. PREPARE
1. RECON
3. EXECUTE



Conclusion

Your bank account has been targeted and you need to provide certain details, so the problem can be eradi

---

Baiting – Diana Maldonado Luberto

Introduction

Baiting is one of many forms of social engineering that is found now a days. It is typically an attack

Content

1. Who do they mainly attack?
2. What is the main promotion maybe?
3. What are possible ways to not fall under baiting?

Conclusion

`Overall social engineering builds up about 98% of the cyber-attacks world-wide basically meaning that al`

Scareware – Annabel Mejia Cortes

Introduction

`Scareware is a form of social engineering where the technique used is to give people viruses by creatin`

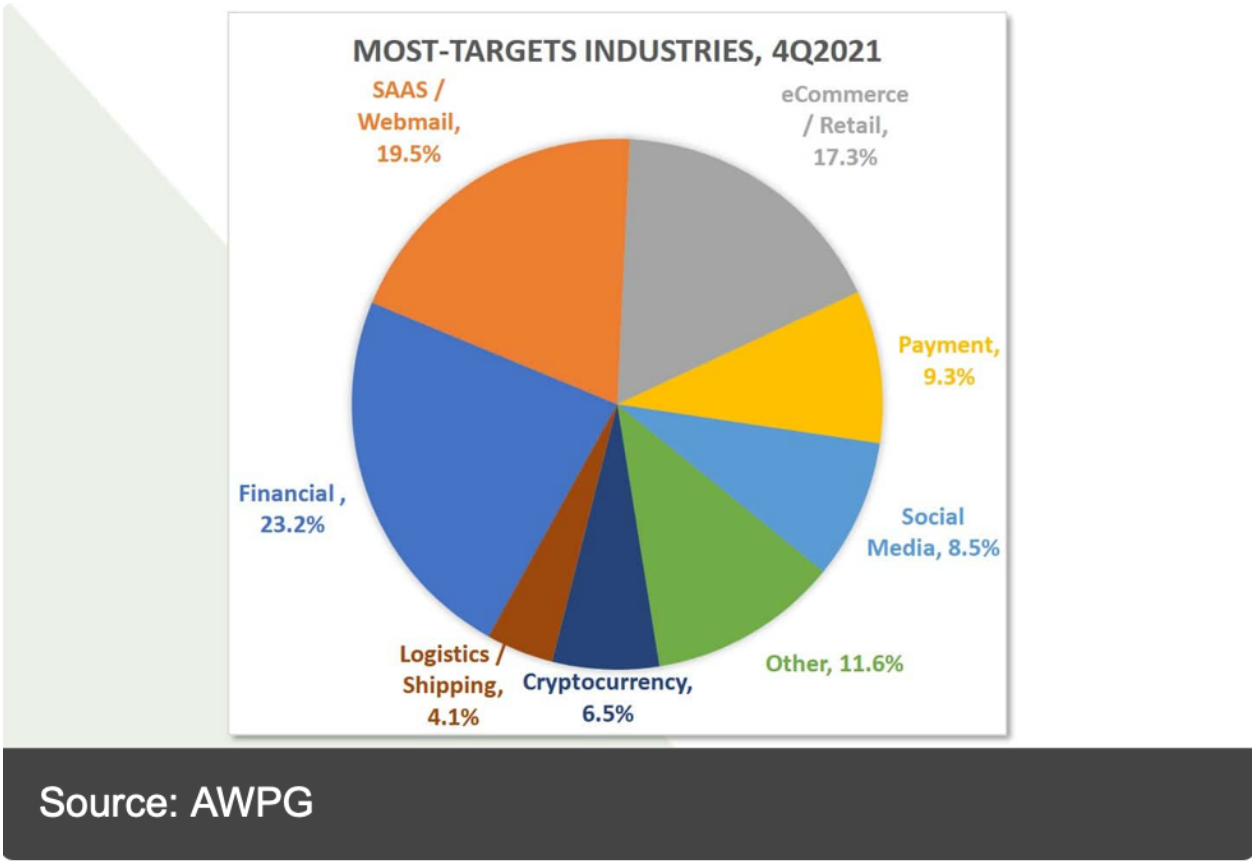
Content

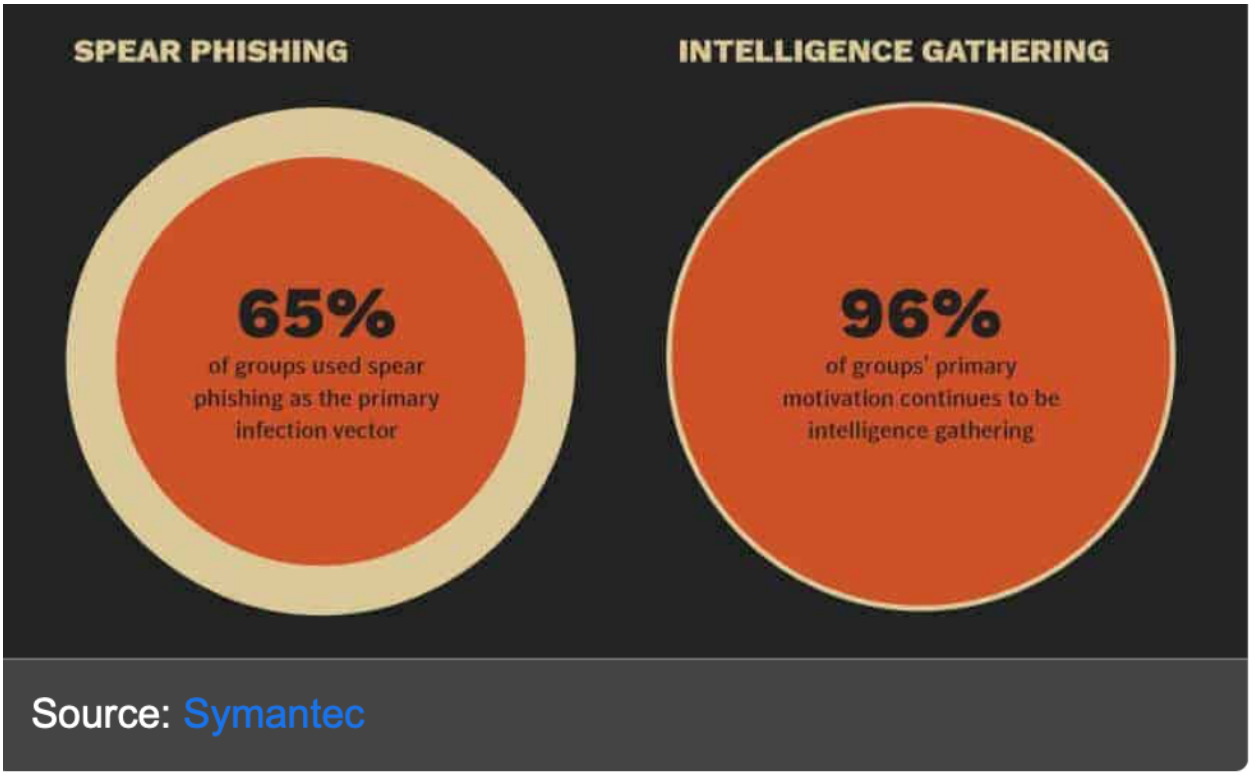
1. Different methods of scareware tactics

- Pop-ups disguised as protection plans
- Ads shown on trusted websites
- Pop-ups telling you there have been viruses detected on your device

2. How to identify scareware tactics

- Check the URL as often people will use a very similar URL to that of a legitimate website.





Conclusion

This form of cyber-attack is still very prominent in our current society, and with technology being comm

---

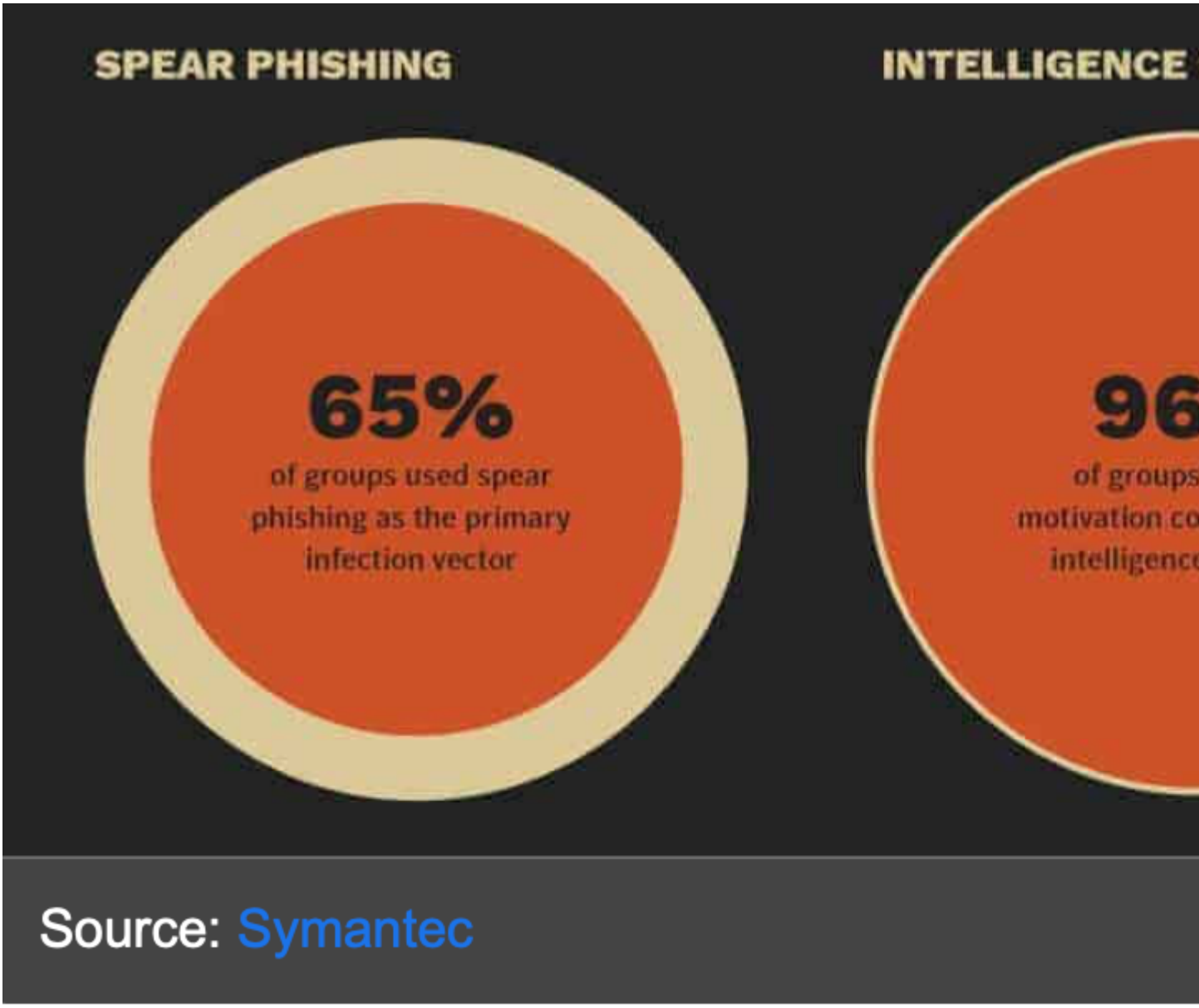
Phishing – Carmen Lopez

Introduction

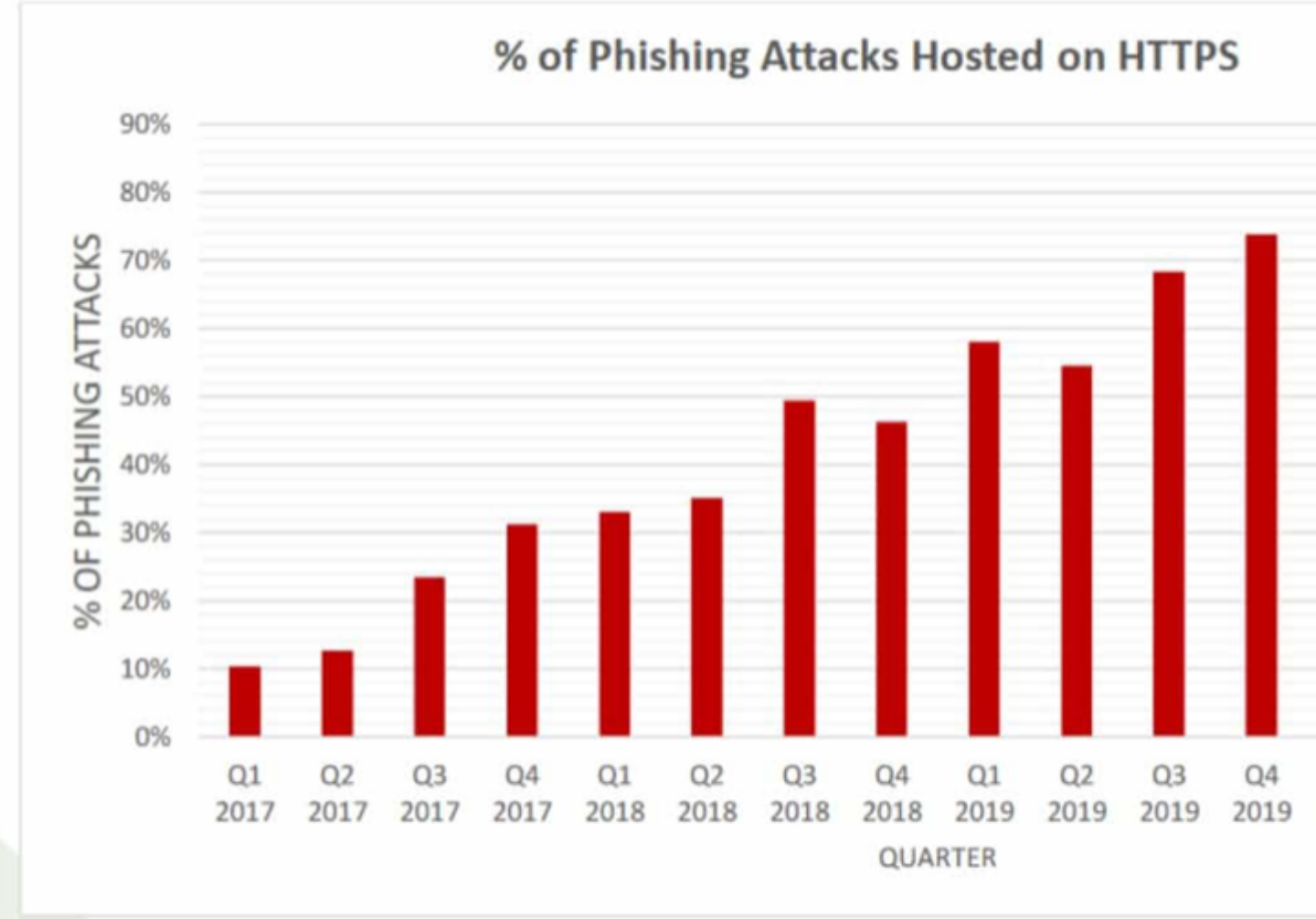
Phishing is the act of sending messages, emails, letters, ect. In a way to pass of as a reputable compar

Content

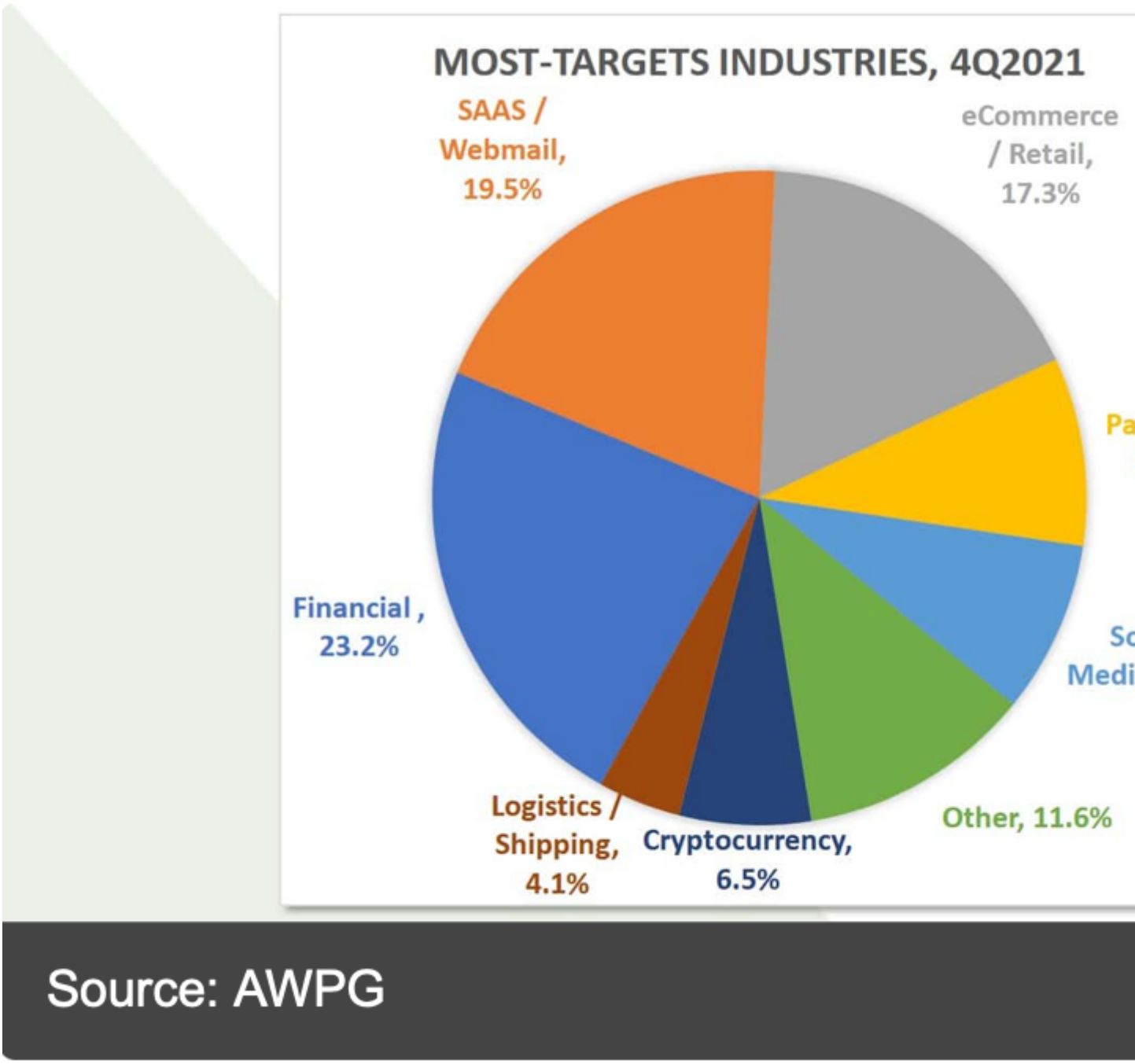
1. What are the main reasons hackers choose phishing as a way to attack?
2. Who are the most targeted?
3. How much has Phishing grown in the USA?



Source: Symantec


% of Phishing Attacks Hosted on HTTPS
% OF PHISHING ATTACKS
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Q1 2017
Q2 2017
Q3 2017
Q4 2017
Q1 2018
Q2 2018
Q3 2018
Q4 2018
Q1 2019
Q2 2019
Q3 2019
Q4 2019
QUARTER

Source: APWG



Conclusion

Years continue to go by, and phishing will also continue to grow as the attackers tend to get more and m

---

Quid Pro Quo – Austin Mercado

Introduction

From the various ways of social engineering, one of the infamous styles that wrecks much havoc across t

Content

1. Real Life Scenarios examples of Quid Pro Quo
2. Ways to avoid Quid Pro Quo.

Conclusion

1. More than ever, social engineer attacks have been at their highest more than ever. Quid Pro Quo is a potential dangerous trade that results in millions of dollars of value stolen. In addition, the development of further trouble ahead in life that comes to affect many in the long run. The best way to avoid harm to oneself or another is acknowledge1qxx the problem and make awareness of the scheme of Quid Pro Quo that has developed in this world.