

Social Engineering

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

2023-04-22

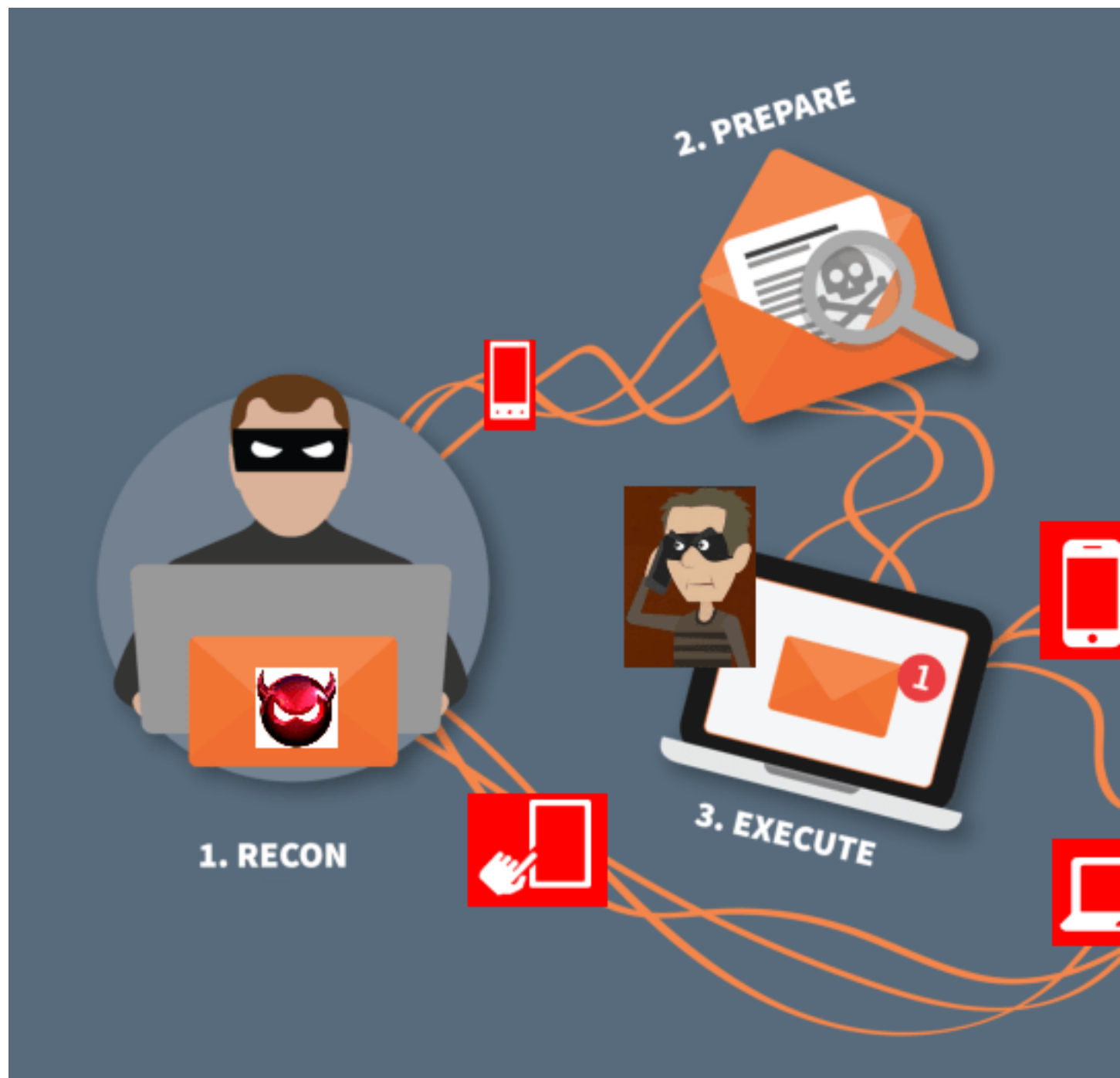
Pretexting – Jocelyn Morales

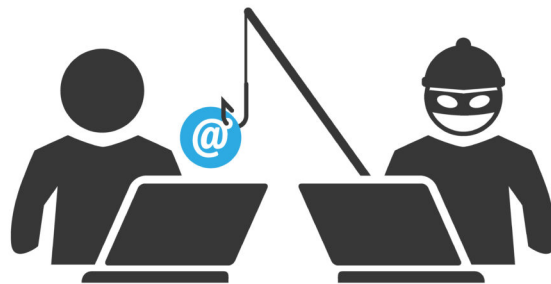
Introduction

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.





Conclusion

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

Sources

- Social engineering attack examples, templates, and scenarios
- OmeTV Pretexting Phishing Attacks: A Case Study of Social Engineering
- Social Engineering: The Looming Threat

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 v

Content

1. Who do they mainly attack?
 - Business employees *Teenagers
2. What is the main promotion maybe?
 - New phones typically include the newest ones on the stock market.
 - Free access:
 - Movies
 - Music
 - Gift Cards
 - False packaging information from a fake FedEx or UPS
3. What are possible ways to not fall under baiting?
 - Antiviruses and anti-malware baiting?
 - Proper network security
 - If offers look to “good to be true” do NOT open the links

Conclusion

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





Sources

- Privacy Sense.net: Baiting
 - Don't Take the Bait! Phishing and Other Social Engineering Attacks
 - What is Baiting in Cybersecurity? Techniques, Examples, Protection
-

Scareware – Annabel Mejia Cortes

Introduction

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

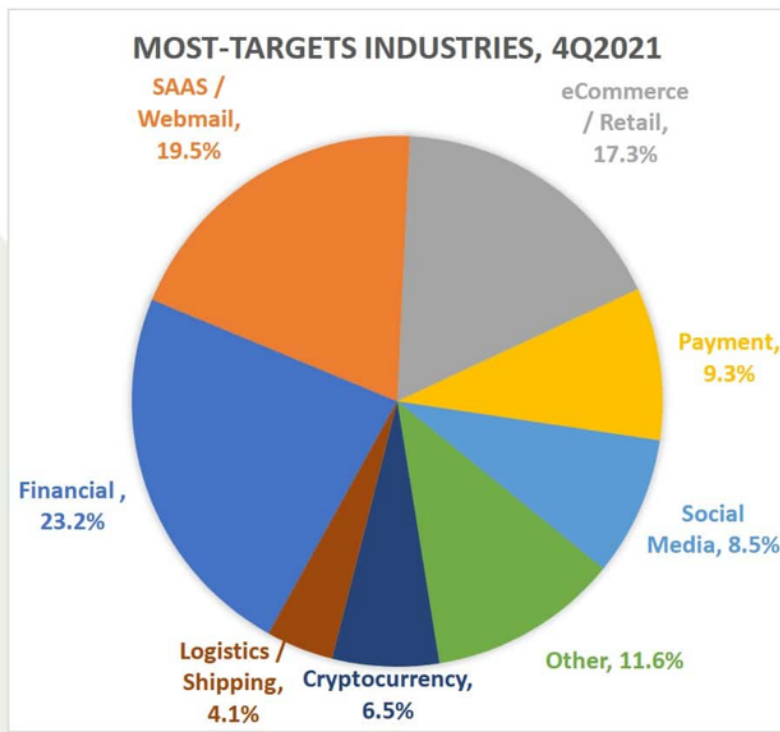
Content

1. Different methods of scareware tactics

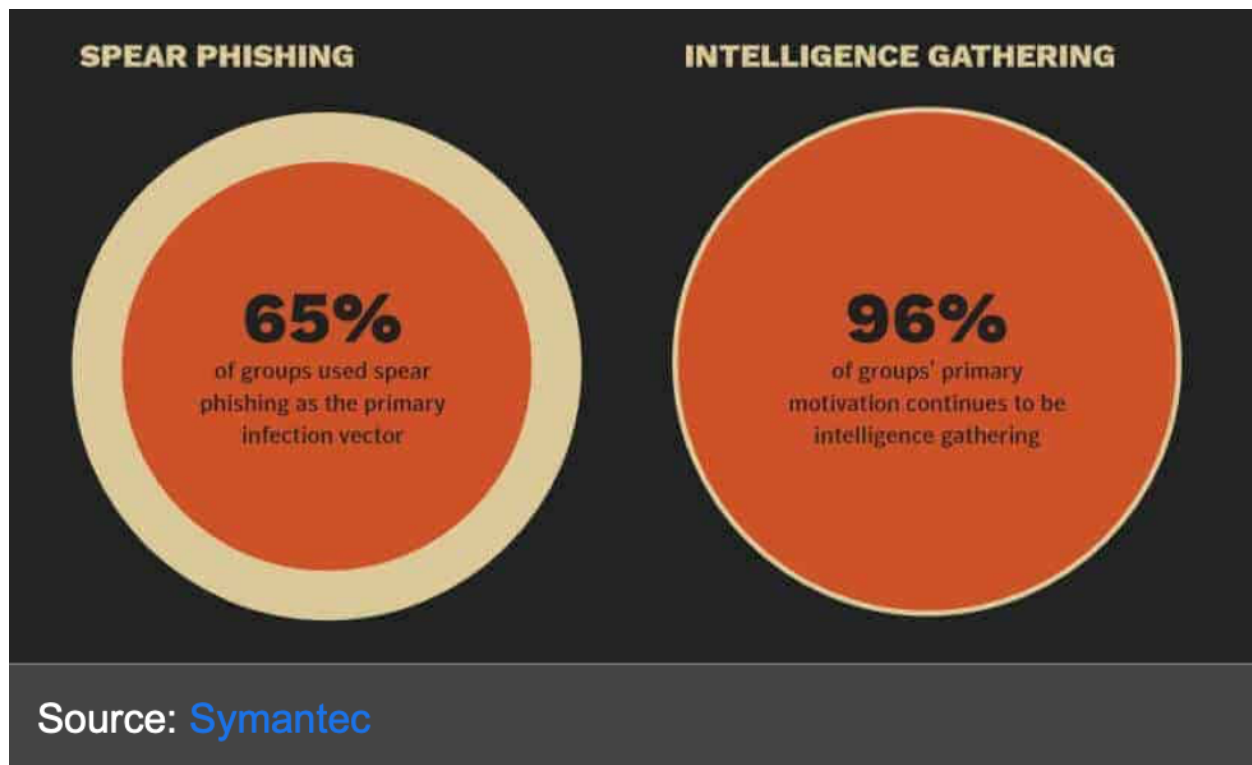
- Pop-ups disguised as protection plans
- Ads shown on trusted websites
- Pop-ups telling you there have been viruses detected on your device
 - They can look very real when they are custom made to look like the software you are using.
 - Note that an advertisement doesn't scan for viruses without you allowing them.

2. How to identify scareware tactics

- Check the URL as often they will use a very similar URL to that of a legitimate website
- Unfamiliar company name
- Urgency from the pop-up
- Difficult to find the 'x' button to discard the pop-up
- Starts with "Warning!" or Virus detected!



Source: AWPg



Source: [Symantec](#)

Conclusion

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

Sources

- Social Engineering: What is Scareware?
 - Protection against Semantic Social Engineering Attacks
 - Sizing up the malware threat
-

Phishing – Carmen Lopez

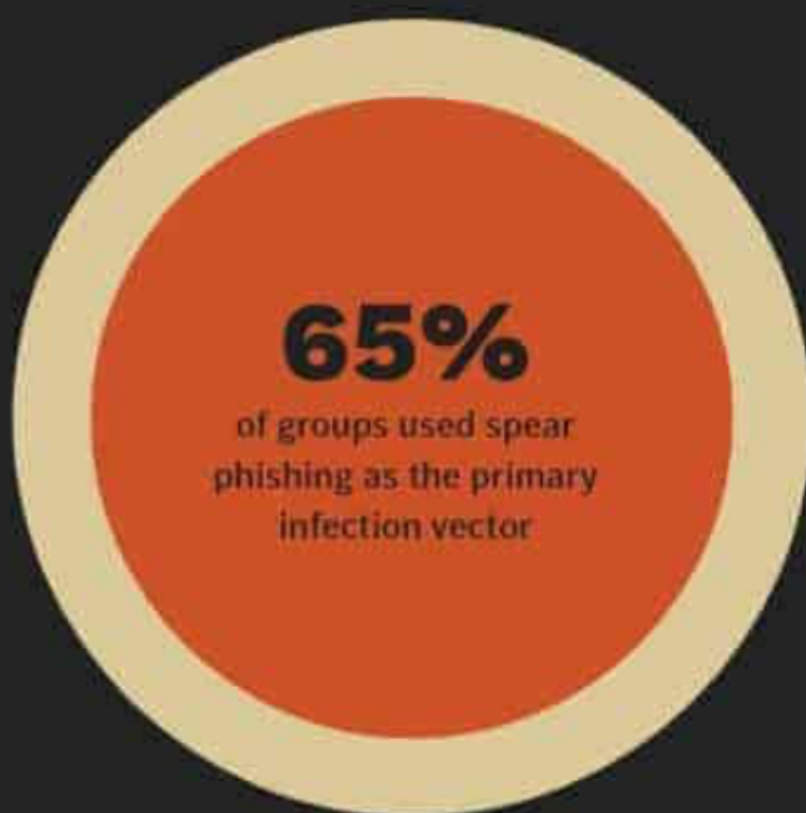
Introduction

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

Content

1. What are the main reasons hackers choose phishing as a way to attack?
 - The reason why many attackers choose phishing as a way to attack is because it is easy to fool people into clicking their link. Many people tend to be gullible when they see a message saying they won free tickets and can't help but click the link attached. This simple action causes for all personal data to be hacked.
2. Who are the most targeted?
 - Phishing attackers attack employee's of all company levels. This is to be able to steal as much information from them as possible including company financial statements and employee information.
3. How much has Phishing grown in the USA?
 - Phishing is the most common form of cyber attacks with over 3.84 billion attacks a day. Recently there has been a 61% growth rate in the United States from phishing emails which is a huge jump.

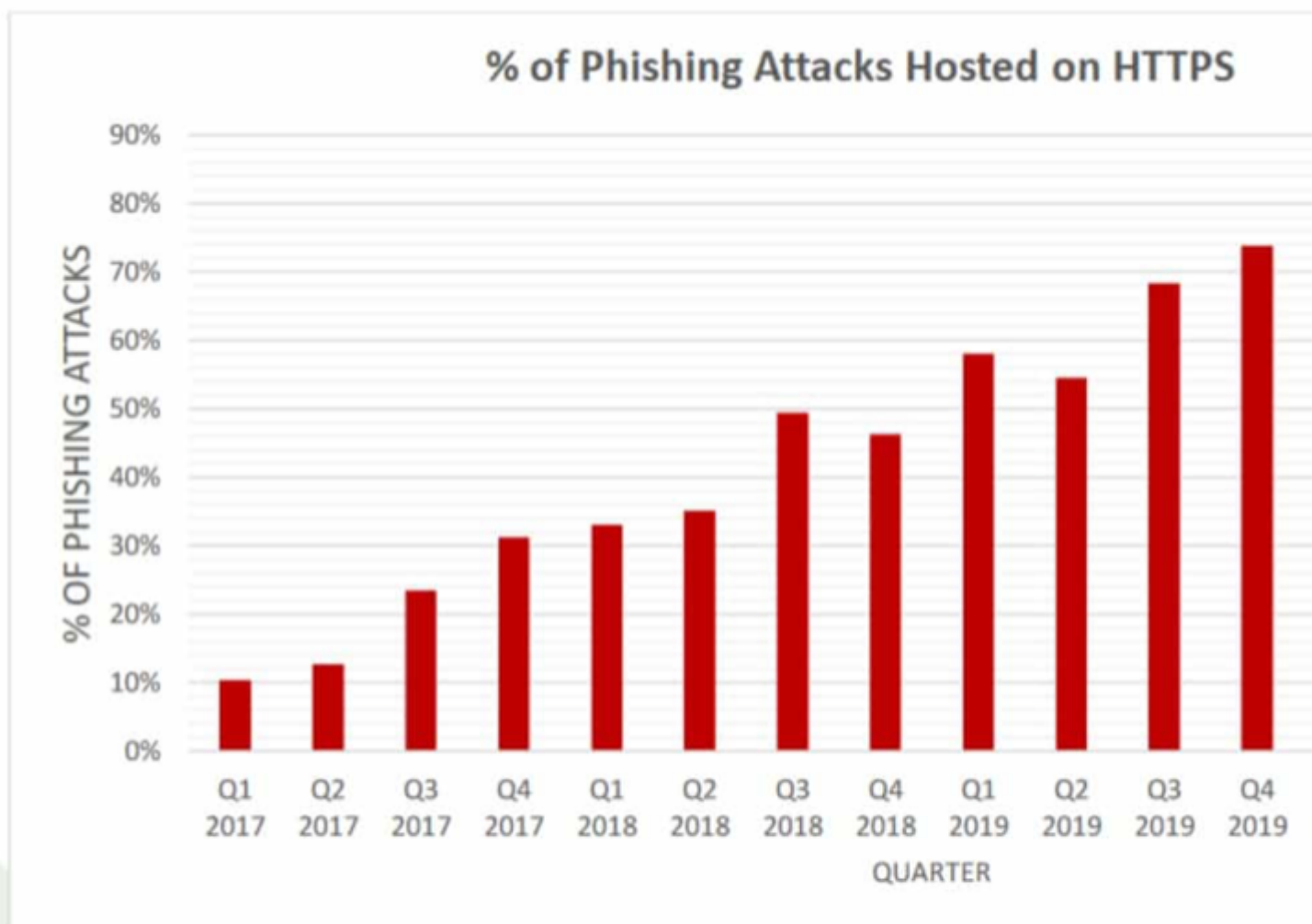
SPEAR PHISHING



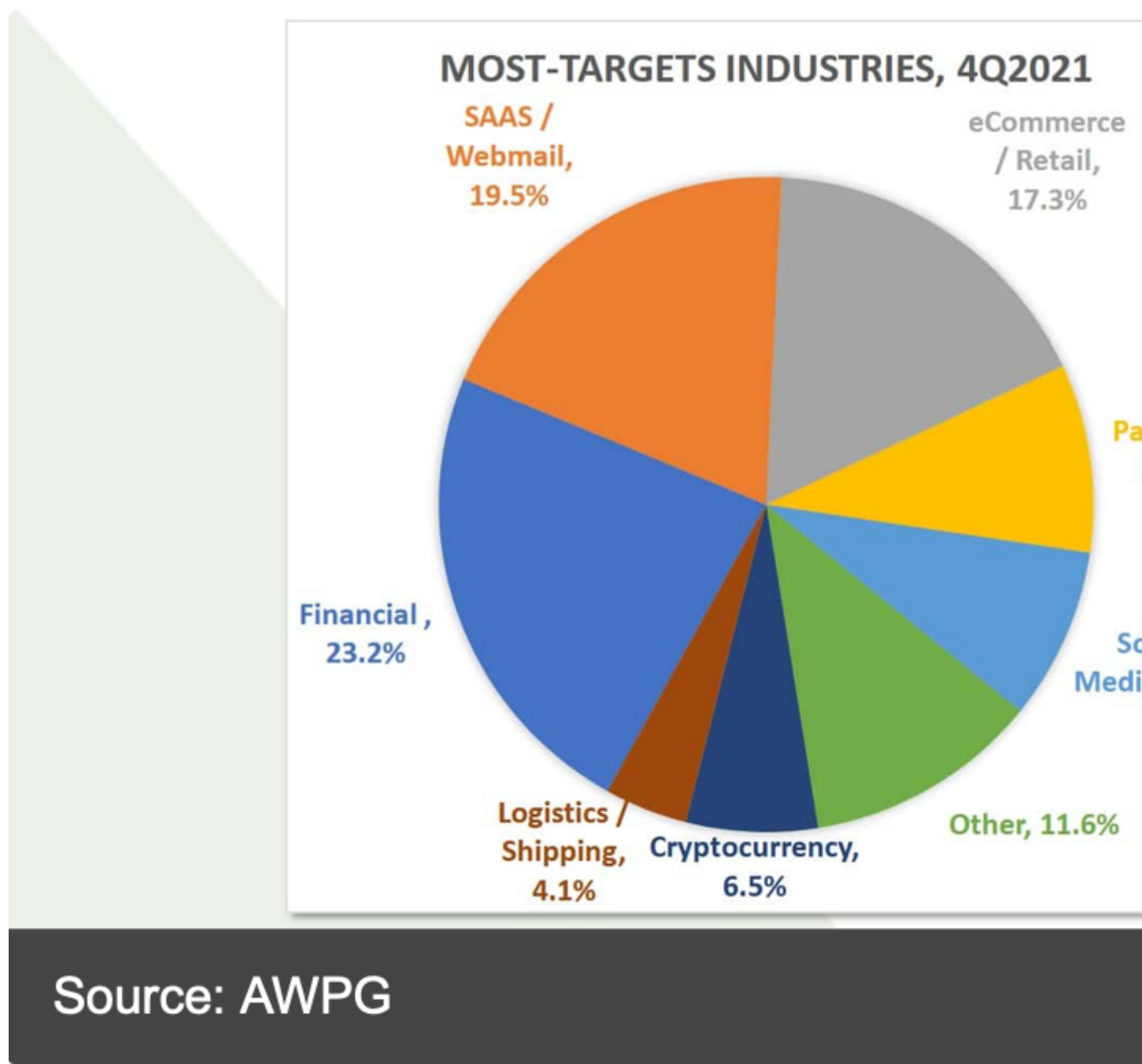
INTELLIGENCE



Source: [Symantec](#)



Source: APWG



Conclusion

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

Sources

- ScienceDirect: Phishing-challenges and solutions
- Confense: History of Phishing
- CSUSB ScholarWorks: A Study of Social Engineering Concepts Within A Deceptive Defense

Quid Pro Quo – Austin Mercado

Introduction

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

Content

1. Early Signs of Quid Pro Quo:

- Bad Gut feeling
- Feeling of “too good to be true”

2. Ways to avoid Quid Pro Quo:

- Request help from someone close or second opinion before engaging a possible Quid Pro Quo.
- Request contact information or stall till confirmation
- Look into it before following the instructions
- Look at the fine lining





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 acknowledge the problem and make awareness of the scheme of Quid Pro Quo that has developed in this world.

Sources

- ScienceDirect: Overview of Social Engineering Attacks on Social Networks
- AIS eLibrary: A Taxonomy for Social Engineering attacks
- International Journal on Advances in Engineering, Technology and Science, Protection of Computer Networks from the Social Engineering Attacks