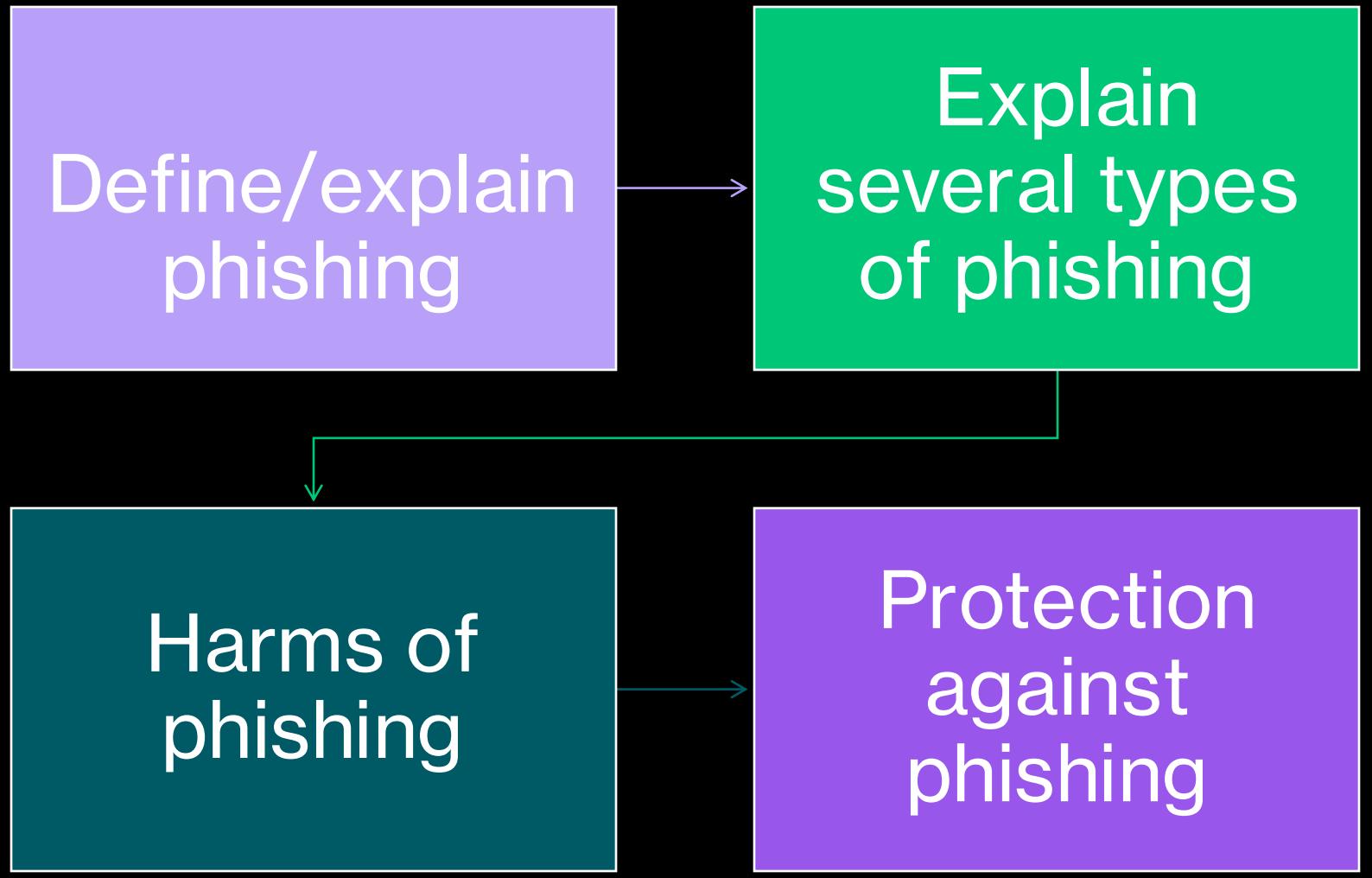
Phishing

Gabe Olivier and Mario Pomorski

Objectives


Define/explain phishing
Explain several types of phishing
Harms of phishing
Protection against phishing

Quick Facts

Phishing is the most common form of cyber crime

+ ~3.4 billion spam emails are sent everday
+ Every ~11 seconds a phishing email is sent
+ 1/5 of phishing emails come from Russia

Phishing is lucrative

+ On average ~$4.91 million in breach costs
+ Largest attack was ~1.8 billion

What is Phishing?

Definition:

The fraudulent practice of sending emails or other messages to induce individuals to reveal personal information, such as passwords and credit card numbers.

Types:

1. **Spear Phishing**
2. **Vishing**
3. **Angler phishing**
4. **Quishing**

Spear Phishing

Strategy:

Targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents

Method:

Messages are delivered via e-mail and are designed to convince the user to open a malicious link or attachment.

Spear Phishing Example

Subject Line: Quarterly Report

Dear Mario Pomorski,

I noticed that you have not yet submitted your quarterly report. Attached is a template for the report, please fill this out immediately.

I expect a full analysis by the end of the day,
Gabe Olivier

Tec Corporations CEO

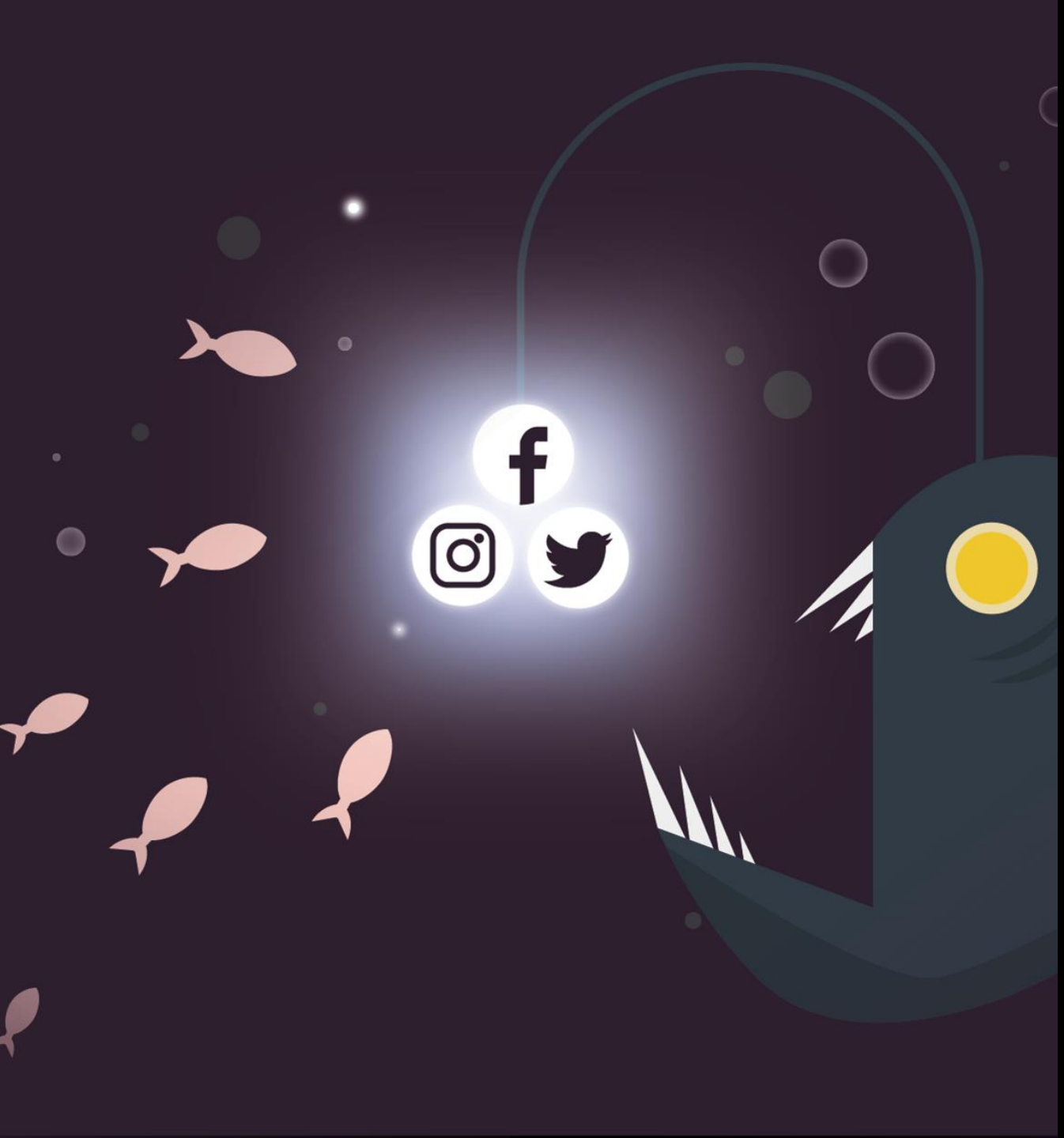
Vishing

Strategy:

An attack where scammers use phone calls to stress individuals into revealing personal information.

Method:

This type of scam can be executed by real humans or via pre-recorded robocalls. They also often leave voice messages to increase their chances of success.



Angler phishing

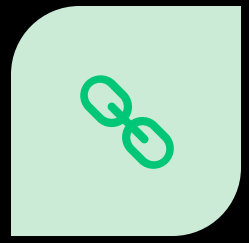
- **Angler Phishing** is a type of cyberattack where **fraudsters impersonate customer service accounts** on social media platforms to trick users into giving up sensitive information.
- The term “angler” comes from **angling (fishing),** the attacker “baits” users by posing as legitimate support representatives.

Why it's Effective

- **Timely and targeted**: Attackers monitor hashtags and mentions in real-time.
- **Looks legitimate**: Fake accounts often use company logos and names that are hard to distinguish from the real ones.
- **Urgency**: The attacker may claim immediate action is needed to fix the issue.
- **Trust in brands**: Users expect helpful, fast replies from customer service.

How to Stay Safe

VERIFY ACCOUNTS: ONLY RESPOND TO **VERIFIED** OR OFFICIALLY LINKED SUPPORT ACCOUNTS.



DO NOT CLICK UNKNOWN LINKS IN DMS OR REPLIES.

GO TO THE COMPANY'S WEBSITE DIRECTLY FOR HELP.

BE SKEPTICAL OF URGENT REQUESTS OR REWARD OFFERS.

REPORT FAKE ACCOUNTS TO THE PLATFORM.

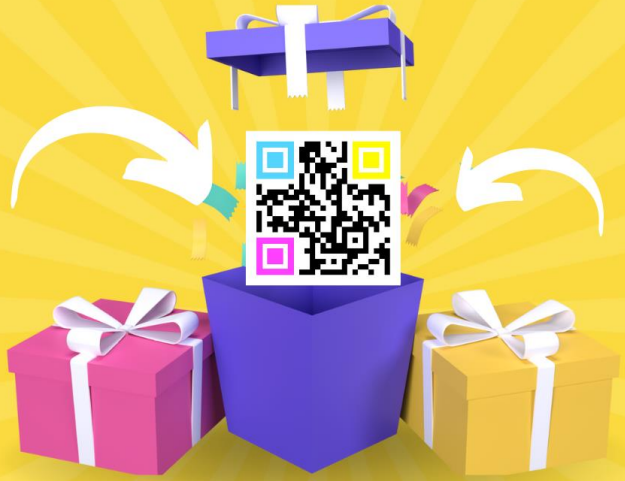
Quishing

- **Quishing** is a form of phishing that uses **QR codes** to deceive users. The term combines “**QR**” and “**Phishing**.”
- Once scanned, the QR code could lead to:
- Fake login pages
- Malware downloads
- Fraudulent payment portals

Special

Giveaway Alert

Million Dollar Cash Prize



- Follow our GETMONEY Instagram account
- Share this post on your Instagram story
- Comment, Like, and tag 5 friends

The winner announcement on

2 Minutes

@reallygreatsite

Why is it dangerous

Invisible URLs: Users can't see the link before scanning.

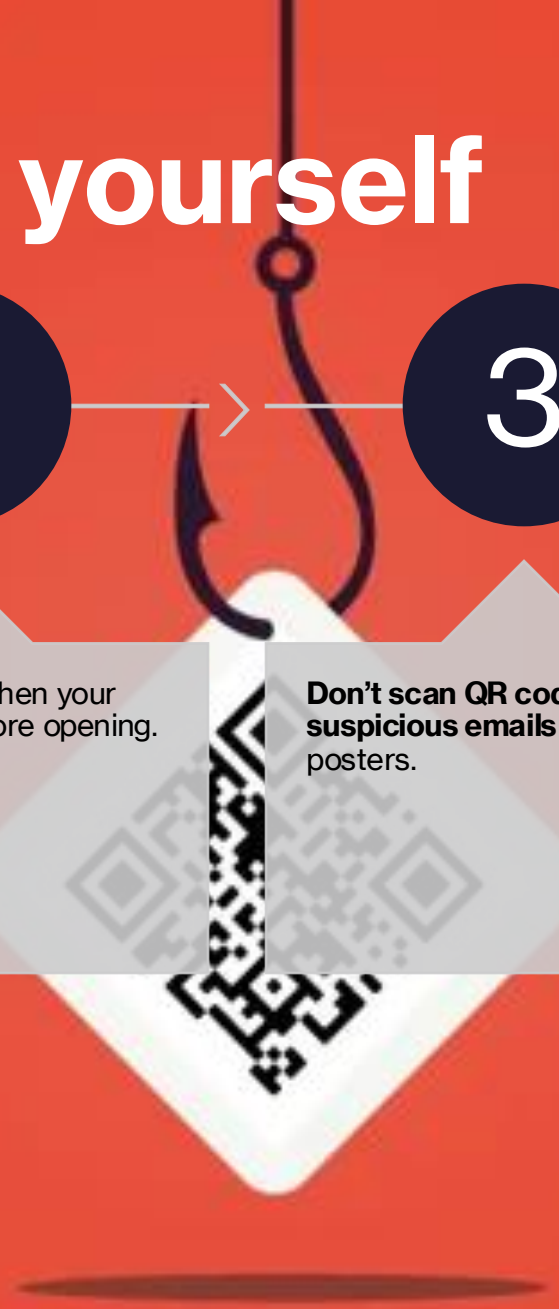
Bypasses filters: Many email security systems don't flag QR codes.

User trust: People often scan QR codes without caution, especially in public places.

No antivirus trigger: A camera scan bypasses traditional desktop protections.

How to protect yourself

1. **Inspect the source** before scanning any QR code.
2. **Preview the URL** when your phone shows it before opening.
3. **Don’t scan QR codes in suspicious emails** or random posters.
4. **Use QR scanning apps** that show full URLs before redirecting.



References

- https://www.terranovasecurity.com/solutions/security-awareness-training/what-is-vishing
- https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Spearphishing.pdf
- https://aag-it.com/the-latest-phishing-statistics/
- https://news.usps.com/2024/06/19/if-you-dont-know-about-quishing-read-this/
- https://www.experian.com/blogs/ask-experian/what-is-angler-phishing-and-how-can-you-avoid-it/