MALTEGO

What you should know about

# PHISHING ATTACKS

**WHAT ARE PHISHING ATTACKS?**

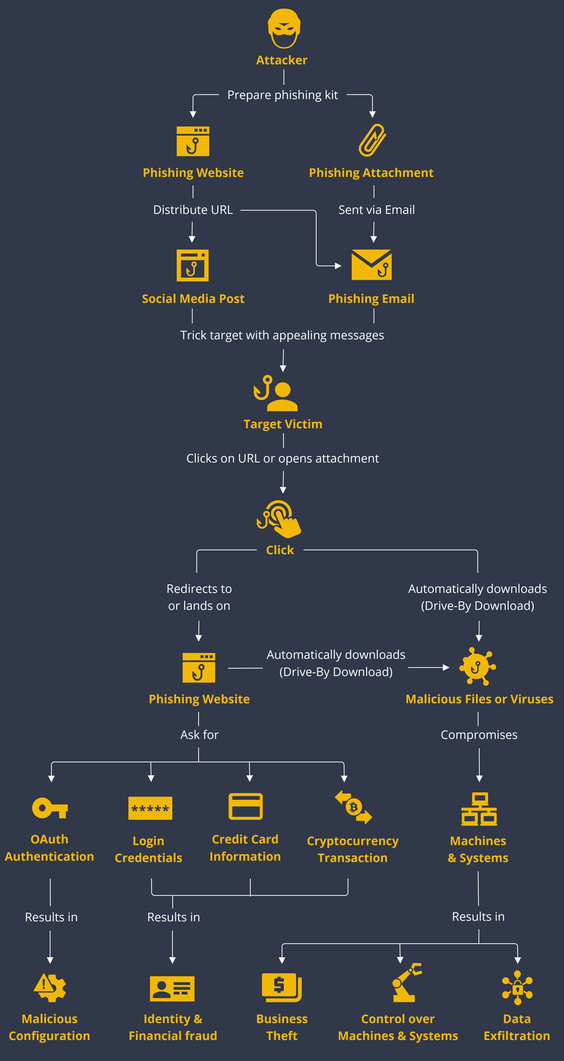
Phishing is a common method used by malicious hackers to steal critical information or infiltrate the target's computer with a malware or virus, and it is achieved by tricking targets into clicking on a URL link or downloading an attachment.

## THE GOAL OF PHISHING ATTACKS

Phishing attacks are often part of larger schemes such as fradulent activities and business compromise. In phishing attacks, hackers try to acquire:

- Personal Identity & Financial Info
- Login Credentials (*****)
- Confidential Business Intel
- Control over Machines & Systems

## ANATOMY OF A TYPICAL PHISHING ATTACK




## HOW TO SPOT & AVOID PHISHING ATTACKS?

**DOPPELGÄNGER**
A copycat of the original website, log-in page, advertisement, social accounts, or newsletter format.

**SHORTENED URL**
Malicious URLs hiding behind shortened versions when posted on social media or sent via Emails. E.g. "bit.ly/12345"

**FAULTY LANGUAGE**
Grammar errors, misspelled words, and over-promising statements.

**ALTERNATIVE TOP-LEVEL DOMAIN**
URLs hosted on uncommon domains such as .ga or .tk or has "multiple" domains.
E.g. "www.i-phishing.com.tk"

**TYPO-SQUATTING**
Misspelled words, extra characters or symbols, or additional words in the phishing URLs or email addresses. E.g. "suupport@maltego.com"

## WHAT TO DO WHEN SPOTTED A PHISHING ATTACK?

1. **Do not click** on the URL or attachment
2. **Report** or mark as spam
3. **Inform** your organization
4. **Use Maltego** to investigate more

**Help everyone stay away from phishing threats by spreading the knowledge of good practices!**

Want to discuss how to investigate phishing threats with Maltego?
**Schedule a personalized demo with us!**

https://www.maltego.com/schedule-a-demo/



#madewithmaltego