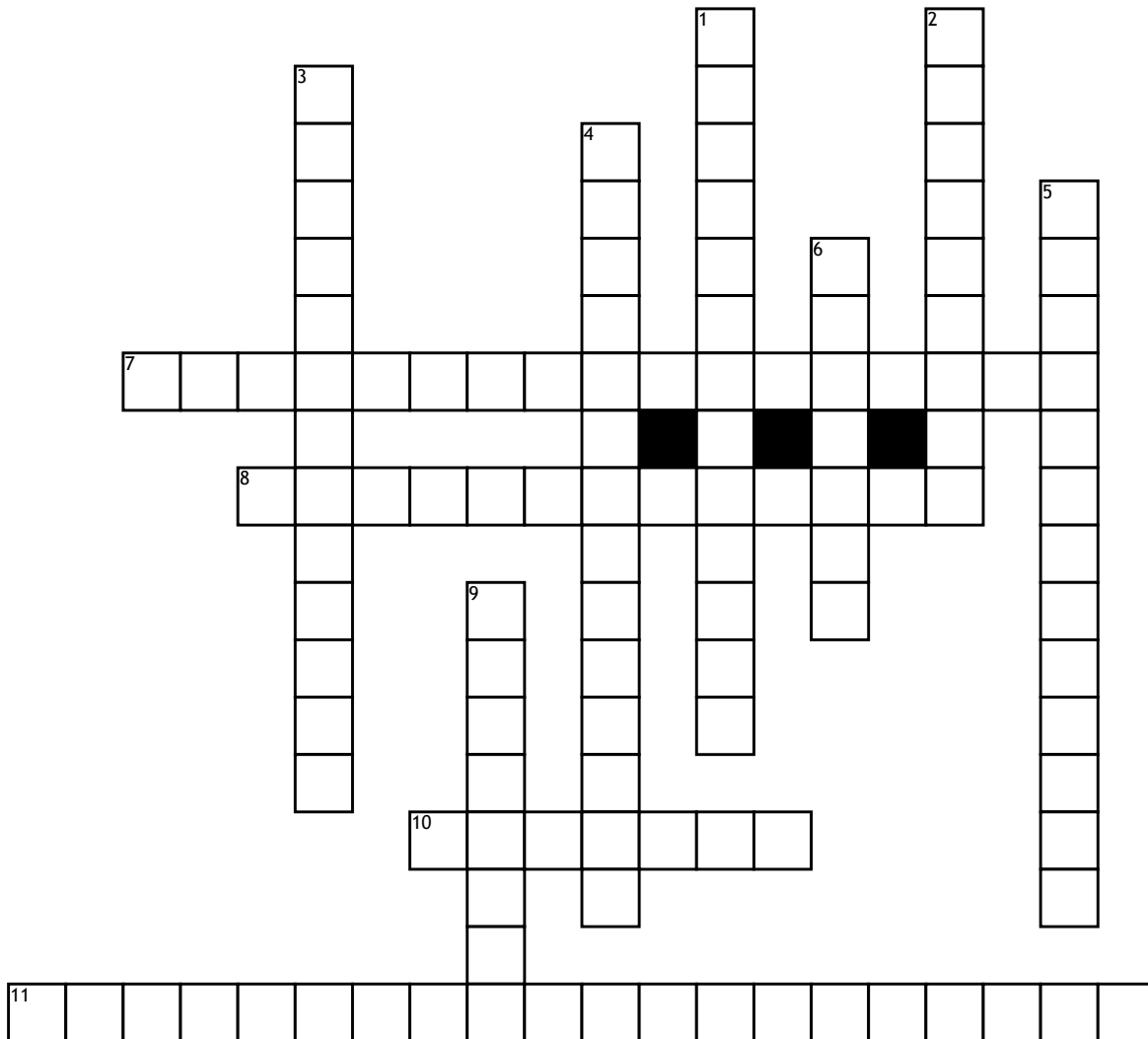# Phishing

Across

7. Attackers get a window to steal the login credentials by redirecting them to a fake website

8. a previously-sent email containing any link or attachment is used as a true copy to create an almost identical email

10. Targets C-suite posts like CEO, CFO, COO – or any other senior management positions

11. Creation of a fake webpage for targeting specific keywords and waiting for the searcher to land on the fake webpage.

Down

1. Targeted in nature, these emails are carefully designed to target a particular user

2. Hackers infect the script of a legitimate website – which you visit regularly, identified through social engineering – with a script that will redirect you to a phishing page

3. Using domains that sound similar to popular websites, they phish users by creating an identical website, where they ask targets to log in by submitting personal information

4. A malicious actor intercepts online interaction between two parties

5. Attackers use images and other media formats to deliver batch files and viruses

6. Refers to phishing done over phone calls

9. Users may receive a fake DM or fake order detail with a cancellation link