



RECOGNIZE THE DANGERS OF PHISHING

What is Phishing?



Phishing is a cyberattack using email, phone (vishing), or text (smishing) to **trick individuals** into **sharing personal info** with cybercriminals.

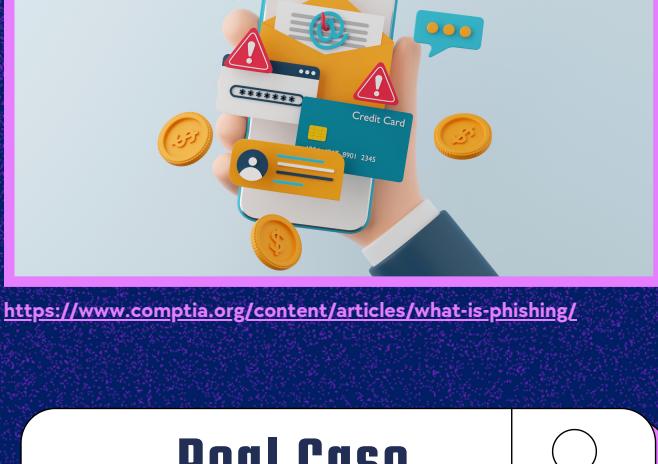


<https://www.comptia.org/content/articles/what-is-phishing/>

Types of Phishing



- **Email Phishing** involves sending fake emails requesting personal information or login details.
- **Smishing** uses fraudulent text messages to gather information, such as credit card details.
- **Vishing** entails fraudulent calls aimed at obtaining sensitive information.



<https://www.comptia.org/content/articles/what-is-phishing/>

Real Case



Someone sends a fraudulent email to the victim, about winning a prize. The email **contains a link** that must be filled in with a **bank card number** or other confidential information that will benefit the attackers and serve them online.

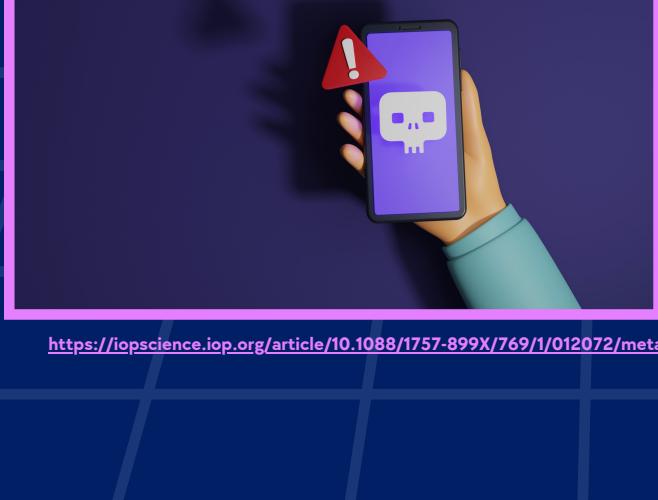


<https://iopscience.iop.org/article/10.1088/1757-899X/769/1/012072/meta>

How to Detect Phishing?



- **User Awareness**
Educating users to **identify phishing attempts**, such as checking website URLs.
- **Software detection**
User-reported blacklists and undisclosed algorithms **identify phishing sites** based on URL and layout. Browser extensions like Google Safe Browsing and McAfee SiteAdvisor detect phishing attempts.



<https://iopscience.iop.org/article/10.1088/1757-899X/769/1/012072/meta>

How to Prevent Phishing?



- Implement Two-Factor Authentication (2FA)
- Utilize Two-Factor Authentication via SMS



<https://iopscience.iop.org/article/10.1088/1757-899X/769/1/012072/meta>