



PHISHING: HOW TO RECOGNIZE AND AVOID SCAMS?

BY : ABIR MAJDI



WHAT IS PHISHING?

Phishing is a cybercrime technique where attackers impersonate legitimate companies to steal sensitive information such as passwords and credit card numbers. These attacks can occur through emails, SMS, phone calls, or fake websites, deceiving victims into revealing their personal data



TYPES OF PHISHING



Email Phishing



Smishing (SMS Phishing)



Vishing (Voice Phishing)



Spear Phishing

SIGNS OF A PHISHING ATTEMPT

Suspicious email addresses

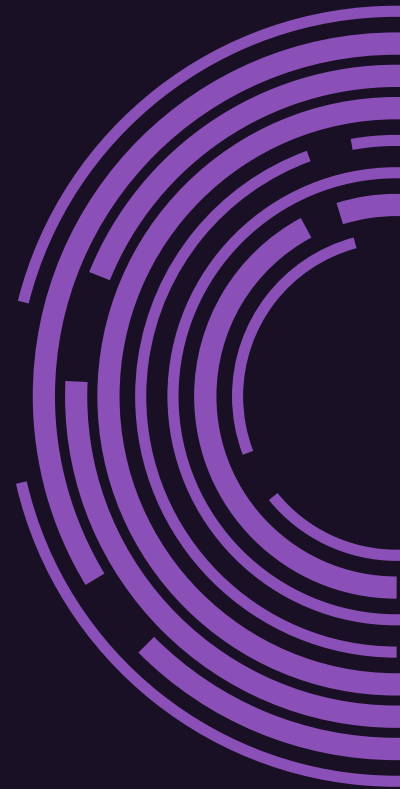
Urgent and alarming
messages

Suspicious links

Requests for sensitive
information

REAL-WORLD EXAMPLE OF A PHISHING EMAIL

1. Fake logo
2. Strange sender email address
3. Suspicious link
4. Message designed to create panic



HOW TO AVOID PHISHING SCAMS?



Never click on suspicious links



Always check the URL before entering credentials



Do not download unknown attachments



CAN YOU SPOT THE PHISHING EMAIL?

Here's an email. Is it phishing or legitimate?



Option 1: Yes, it's phishing!



Option 2: No, it's a legitimate email.

On Fri, Feb 21, 2020 at 11:09 AM
Military Base <usarmybase.mill@mail.com> wrote:
Hello Miss Angie Williams, This is from the military base installation north Carolina, this is to inform you that Joshua Porter is ready to leave the base so he can come to you but you need to send him \$100 as soon as possible or else he's not going to leave the base anymore. Thanks for your understanding

CONCLUSION AND NEXT STEPS



Never share your
sensitive information!



Always stay alert online



Report phishing attempts
to cybersecurity
authorities



USEFUL RESOURCES :

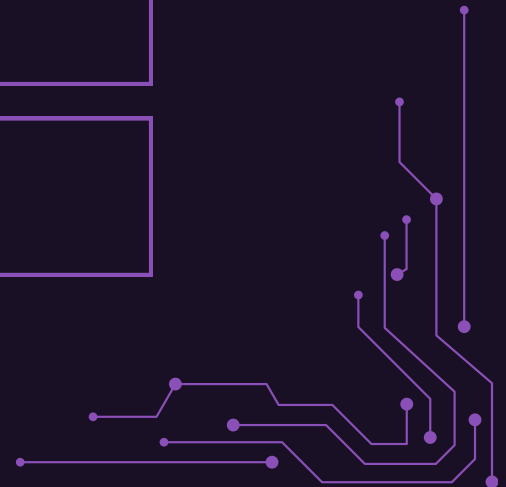
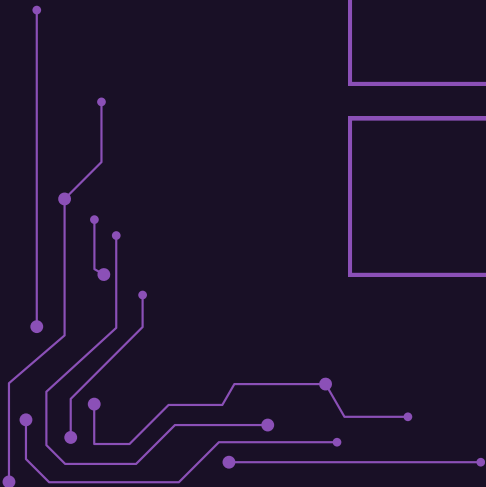


Have I Been Pwned



Cybercrime Support Network

Use VPNs on public networks.





THANK YOU

