Introduction to Social Engineering

- Social Engineering is an act of stealing data from humans. because it doesn't have any interaction with target system or network, it's considered as a non- technical attack. Social Engineering is taken into account because the art of convincing the target to reveal information. it's going to be physically one-to-one interaction with the target or convincing the target on any platform like social media may be a popular platform for social engineering. this is often the very fact that folks are careless, or unaware of the importance of the precious information they possess.

Phases in a Social Engineering Attack

Social Engineering attacks aren't the complex attack which needs strong technical knowledge. An attacker could be Non-technical personal as defined earlier; it's an act of stealing information from people

- **Research**: Research phase includes a set of data about target organization. it's going to be collected by dumpster diving, scanning websites of the organization, finding information on the web , gathering information from users of the target organization, etc.

- **Select Target** : within the selection of target phase, attacker select the target among other employees of an organization. A frustrated target is more preferred because it are going to be easy to reveal information from him.

- **Relationship:** Relationship phase holds creating a relationship with the target within the way that he couldn't identify the intention actually target are going to be trusting the attacker. More Trust level between target and attacker are going to be easier to extract data.

- **Exploit :** Exploit of relationship by a set of sensitive information like Username, Passwords, network information, etc.

Types of Social Engineering

Social Engineering attacks are often performed by different techniques. Different social engineering attack techniques are classified into the subsequent types: -

Human-based Social Engineering

Gathers Sensitive information by interaction

Computer-based Social Engineering

Social engineering is administered with the assistance ofcomputers

Mobile-based Social Engineering

It is administered with help of mobile applications

Introduction of Insider Threats

Social Engineering isn't all a few person gathering information about your organization. it's going to be an insider, an employee of your organization having privileges or not, spying on your organization for malicious intentions. Insider attack is a attacks which are conducted by these insiders. These insiders could also be supported by the competitor of a corporation . A competitor may support an individual in your organization for revealing sensitive information's and secrets.

There are 5 Types of Insider threats Types:

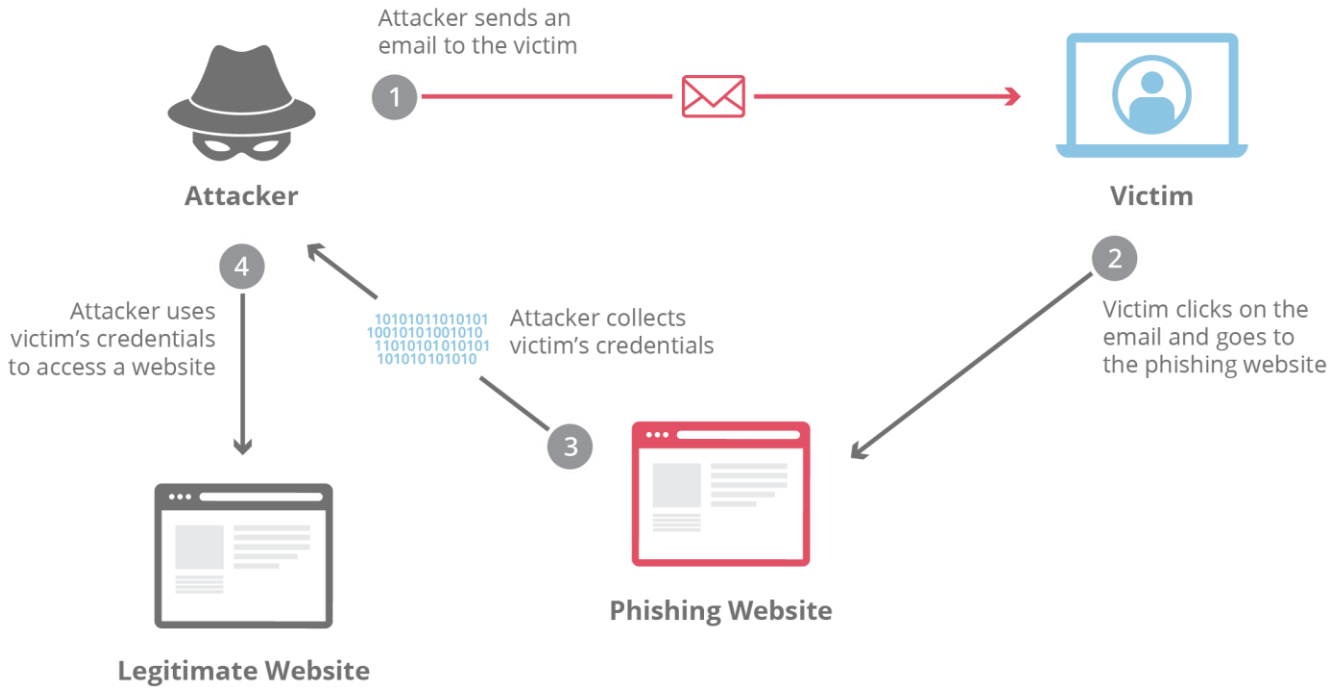
1. Non-responders
2. Inadvertent Insiders
3. Insider Collusion
4. Persistent Malicious Insiders
5. Disgruntled Employees

Common Social Engineering Targets & Defense Strategies

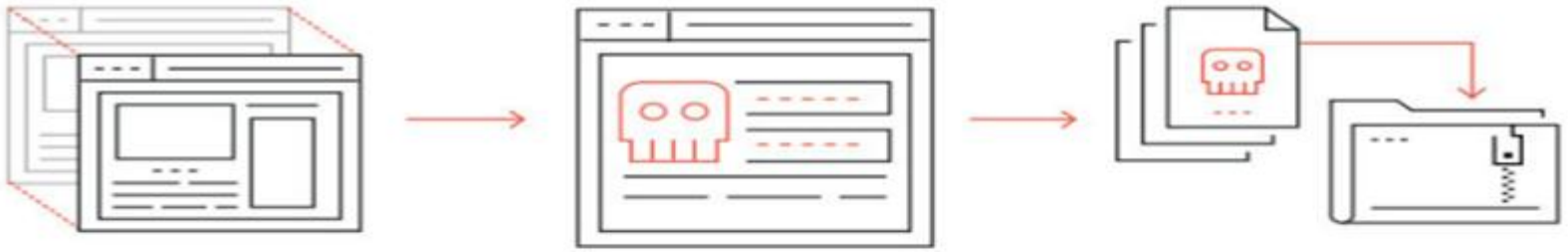
Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk 	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees/help desk to never reveal passwords or other information by phone
Perimeter security 	Impersonation, fake IDs, piggy backing, etc.	Implement strict badge, token or biometric authentication, employee training, and security guards
Office 	Shoulder surfing, eavesdropping, Ingratiation, etc.	Employee training, best practices and checklists for using passwords Escort all guests
Phone (help desk) 	Impersonation, Intimidation, and persuasion on help desk calls	Employee training, enforce policies for the help desk
Mail room 	Theft, damage or forging of mails	Lock and monitor mail room, employee training
Machine room/ Phone closet 	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment

What is Phishing

Phishing may be a sort of social engineering attack often wont to steal user data, including login credentials and mastercard numbers. It occurs when attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, the recipient is then tricked into clicking a malicious link.



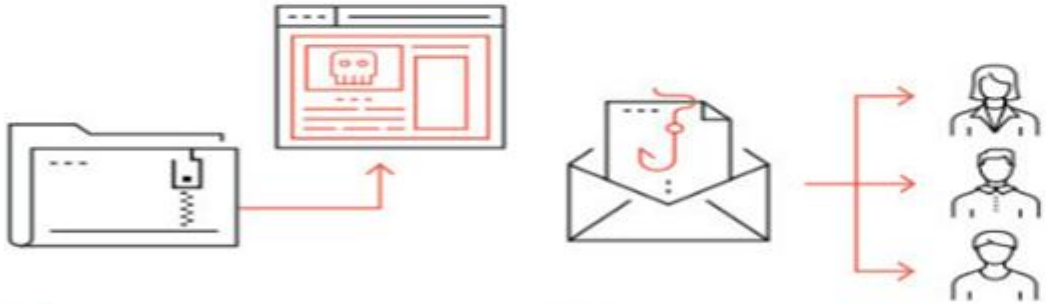
How victims are tricked to access Phishing websites



1.
The legitimate website is cloned

2.
The login page is changed to point to a credential-stealing script

3.
The modified files are bundled into a zip file to make a phishing kit

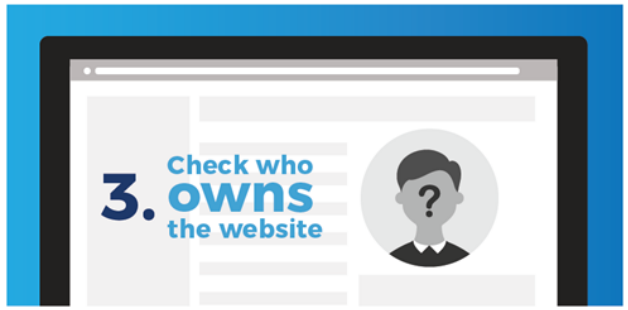


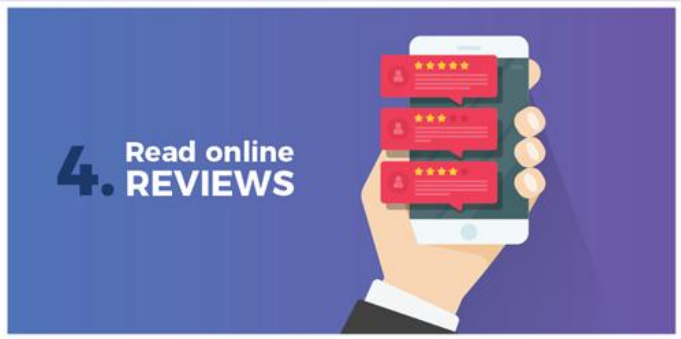
4.
The phishing kit is uploaded to the hacked website, files are unzipped

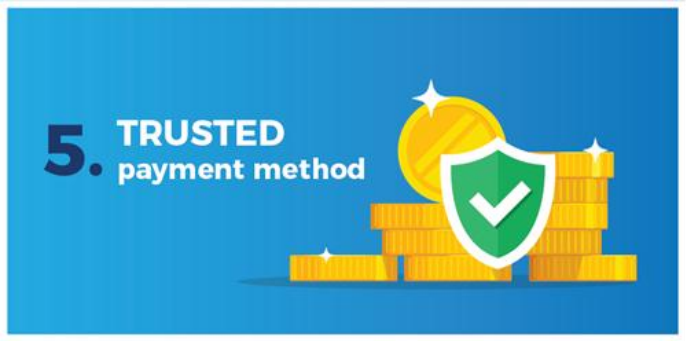
5.
Emails are sent with links pointing to the new spoofed website

How to Differentiate Phishing and original webpage

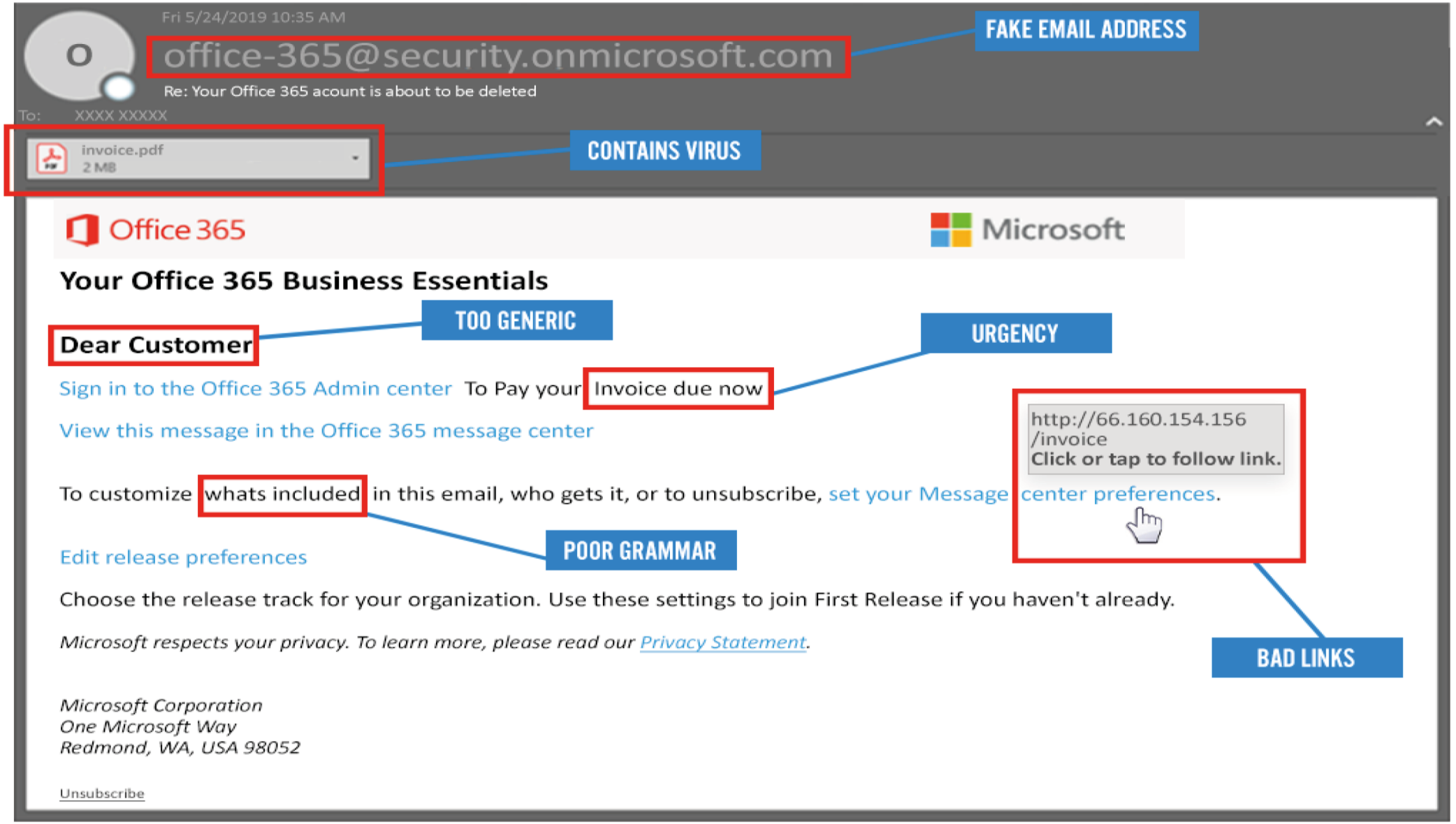
There are 5 ways to differentiate Phishing website and Original website are below







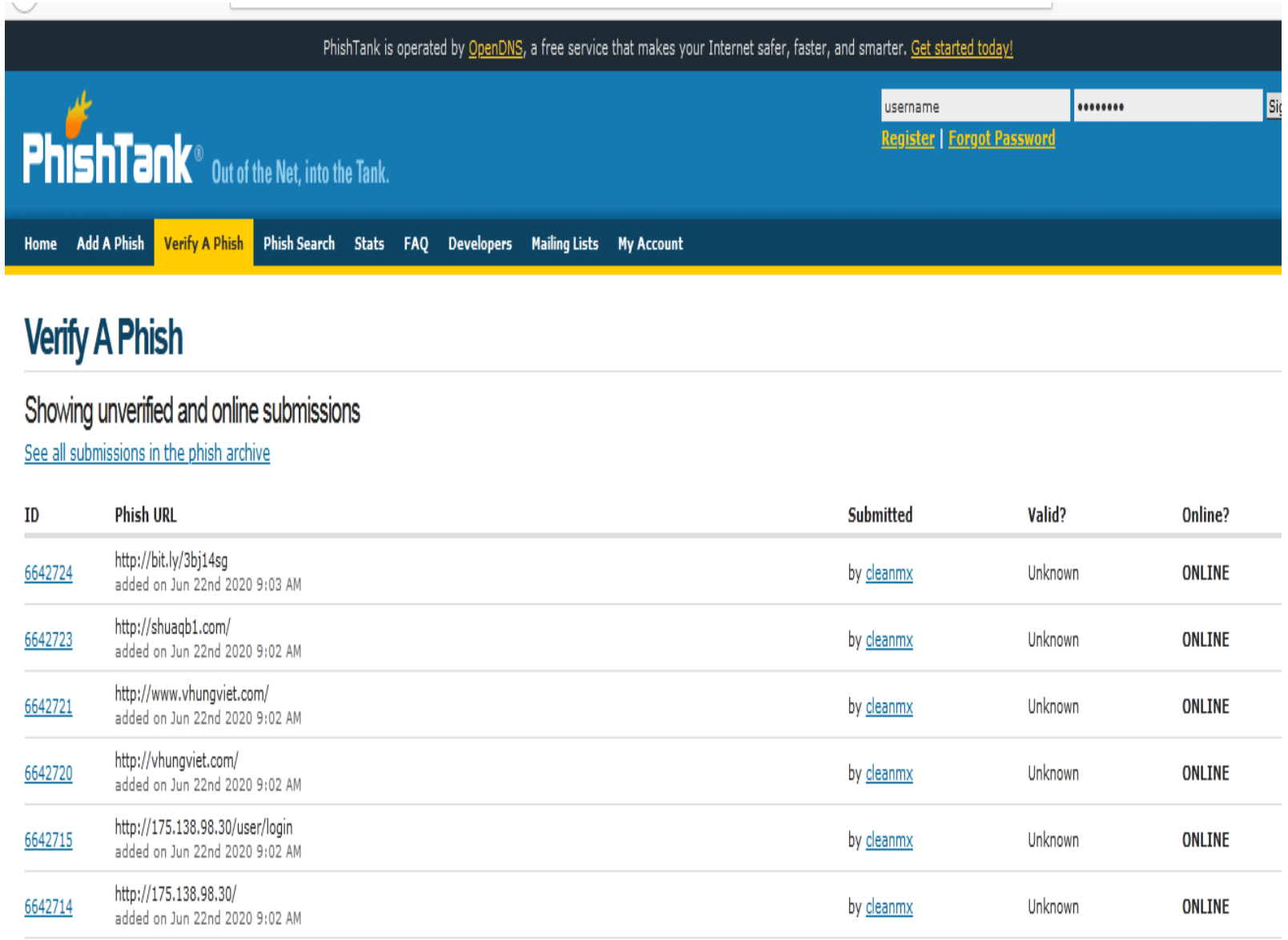
How to Detect Phishing Mails



Tools to Detect Phishing websites: PhishTank

PhishTank is a collaborative clearing house for data and information about phishing sites on the internet

It provides an open API for developers and researchers to integrate anti-phishing data into their applications



How to Defend against phishing attacks

- Never Click on Hyperlinks in Email
- Never Enter Sensitive data in a Pop Up Window
- Verify HTTPS on Address Bar
- Education on Phishing Attacks
- Keep Antivirus Protection Current
- Utilize Anti-Spam Software
- Utilize Anti-Spy Software
- Install and Maintain a Reliable Firewall
- Protect Against DNS Pharming Attacks
- Utilize Backup System Copies