What is Phishing?

Phishing is a type of cyber attack in which attackers impersonate a trusted entity

How Phishing Works?

- **Bait:** The attacker creates a message or website that appears to come from a legitimate source.
- **Hook:** The victim interacts with the fake communication.
- **Capture:** The attacker harvests the victim's data or installs malicious software.

Types of Phishing Attacks

- ## Email phishing

  Scammers create emails that appear legitimate. This is to trick you into providing sensitive information/ or getting you to download malware.

- ## Spear Phishing

  Targets a specific individual, business, or organization. This type of attack uses personalized facts in order to appear real.

- ## Clone Phishing

  Duplication of legitimate emails that were sent from a trusted source with altered information and links that redirects the victim to a malicious or fake website.

- ## Smishing/Vishing

  SMS texts are sent to victims containing links to phished websites.

  Scammers often use caller ID spoofing to make their calls appear to come from legitimate organizations.

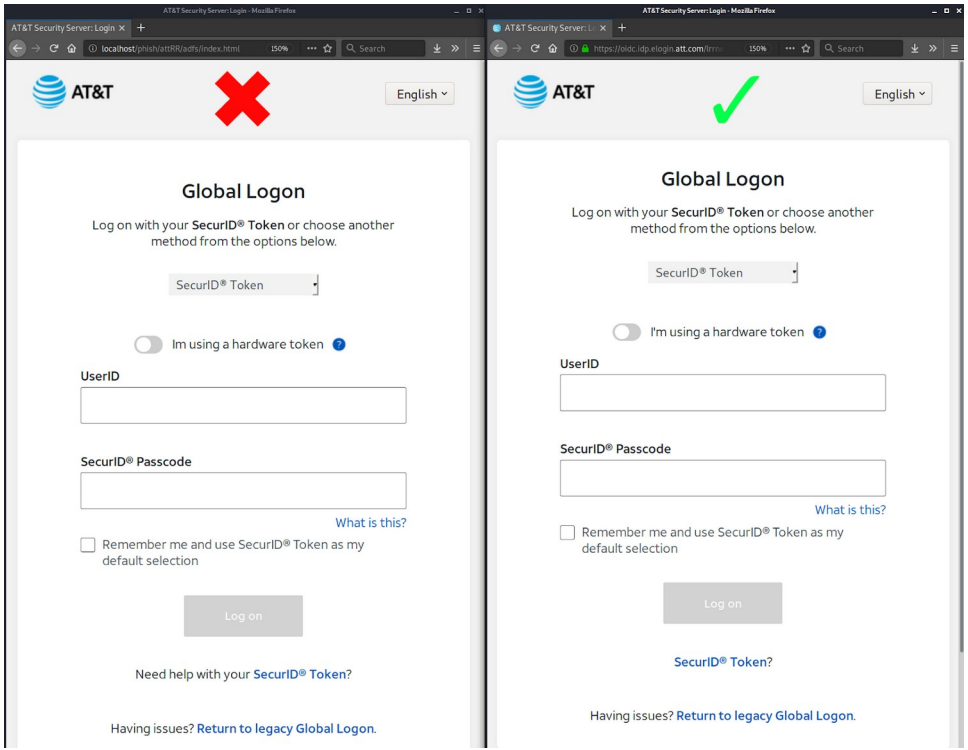
- ## Social media phishing

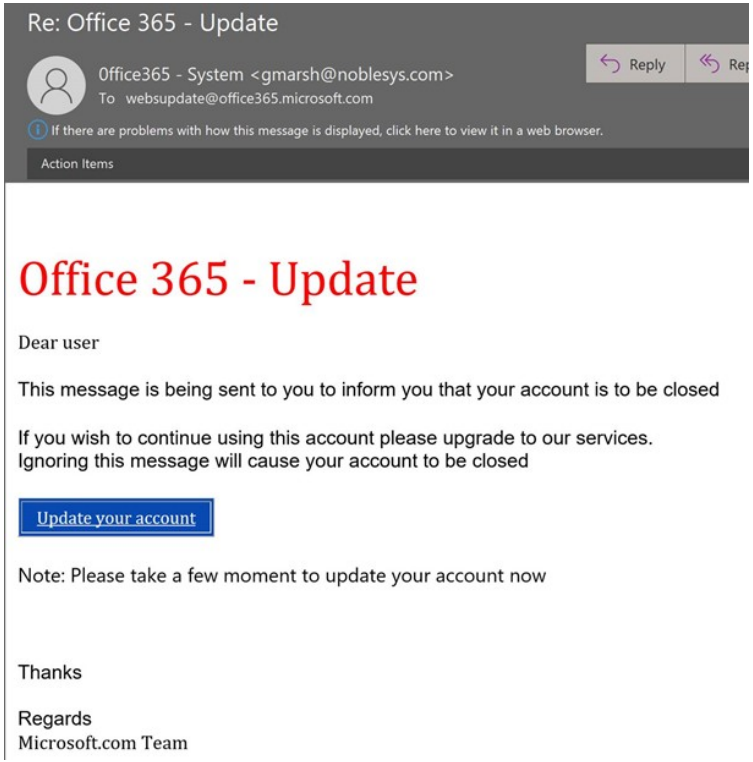
  Scammers use social media platforms to steal personal data or gain control of your social media account.

- ## Website Spoofing

  Fake websites mimicking legitimate ones to steal credentials. Attackers might use link-shortening services to disguise malicious URLs.

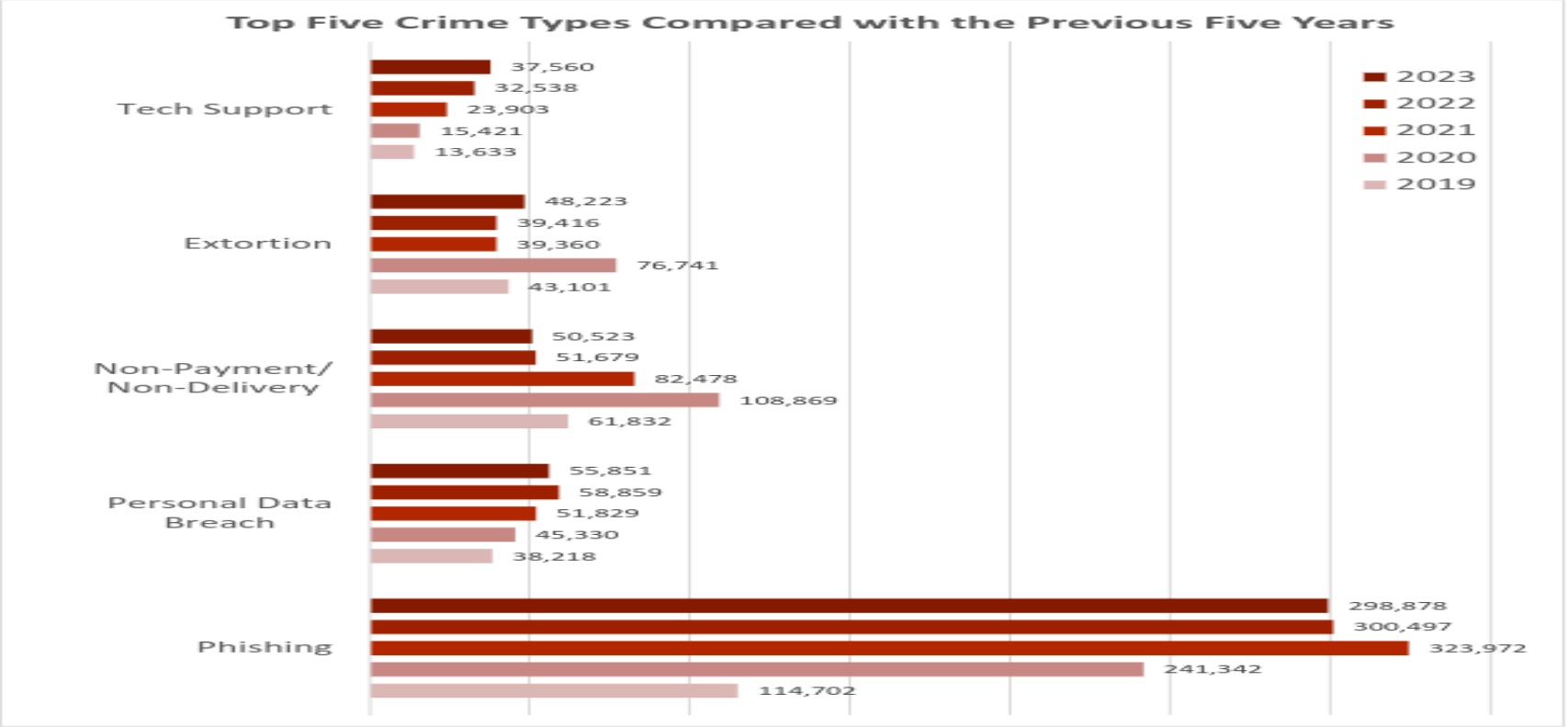
Examples of Phishing





FBI’s Internet Crime Complaint Center (IC3) Statistics

TOP FIVE CRIME TYPE COMPARISON[4]



FBI's Internet Crime Complaint Center (IC3) Statistics

2023 CRIME TYPES

By Complaint Count			
Crime Type	*Complaints*	*Crime Type*	*Complaints*
Phishing/Spoofing	298,878	Other	8,808
Personal Data Breach	55,851	Advanced Fee	8,045
Non-payment/Non-Delivery	50,523	Lottery/Sweepstakes/Inheritance	4,168
Extortion	48,223	Overpayment	4,144
Investment	39,570	Data Breach	3,727
Tech Support	37,560	Ransomware	2,825
BEC	21,489	Crimes Against Children	2,361
Identity Theft	19,778	Threats of Violence	1,697
Confidence/Romance	17,823	IPR/Copyright and Counterfeit	1,498
Employment	15,443	SIM Swap	1,075
Government Impersonation	14,190	Malware	659
Credit Card/Check Fraud	13,718	Botnet	540
Harassment/Stalking	9,587		
Real Estate	9,521		
*Descriptors**			
Cryptocurrency	43,653	Cryptocurrency Wallet	25,815

Real-world Examples of Phishing

- ## Ubiquiti Networks Cyber Scam

  The theft of the $46.7 million via employee impersonation and fraudulent requests.

- ## Sony Pictures Hack (2014)

  Sony executives/CEO received fake Apple ID verification emails.

- ## John Podesta email attack

  Spear-phishing hack was used with an email that looked to have come from Google.

  A total of 33 DNC computers were compromised in the attack.

- ## U.S. Power Grid Phishing Attack

  Attackers targeted contractors and vendors that interact with the grid, using phishing to compromise their systems.

Signs of Phishing

- ## Pressure tactics/Unbelievable deals

  Attackers create a sense of urgency “One time offer” too good to be true.

- ## Requests for $ or sensitive info

  verify the authenticity before providing sensitive information and money.

- ## Poor grammar and spelling

  Many phishing attempts contain grammatical errors and inconsistencies.

- ## Mismatched URLs

  Misspelled URLs or the use of subdomains are common tricks used.

How to Protect Against Phishing

- Verify the sender's identity before clicking on links or opening attachments.
- Enable two-factor authentication (2FA) for accounts.
- Never share your private details with unknown links(IT will not ask for your password).
- Report phishing attempts to your organization or relevant authorities.
- always check the beginning of the website (Look for “https”).

Resource Links

Ubiquiti Networks Attack
Sony Hack
John Podesta Gmail Account Hack
Cyberattack on the U.S. Power Grid
IBM What is Phishing
Internet Crime Complaint Center (IC3) Report 2023