**Common Attacks and Their Effectiveness**

**Phishing**

* **Definition**: Use of digital communications to trick people into revealing sensitive data or deploying malicious software.
* **Types**:
  + **Business Email Compromise (BEC)**: Email from a known source making a legitimate request for information to gain financial advantage.
  + **Spear Phishing**: Targets specific users or groups with emails appearing to be from trusted sources.
  + **Whaling**: Targets company executives to gain access to sensitive data.
  + **Vishing**: Uses voice communication to obtain sensitive information or impersonate a known source.
  + **Smishing**: Uses text messages to trick users into revealing sensitive information or impersonating a known source.

**Malware**

* **Definition**: Software designed to harm devices or networks.
* **Purpose**: Obtain money or intelligence advantage.
* **Types**:
  + **Viruses**: Malicious code that interferes with computer operations and damages data. Needs user initiation.
  + **Worms**: Self-replicating malware that spreads across systems without user initiation.
  + **Ransomware**: Encrypts data and demands payment to restore access.
  + **Spyware**: Gathers and sells information without consent, accessing personal data like emails, texts, and locations.

**Social Engineering**

* **Definition**: Manipulation technique exploiting human error to gain private information, access, or valuables.
* **Types**:
  + **Social Media Phishing**: Collects detailed information from social media to initiate an attack.
  + **Watering Hole Attack**: Attacks websites frequently visited by specific groups.
  + **USB Baiting**: Leaves malware-infected USB sticks for employees to find and install.
  + **Physical Social Engineering**: Impersonates employees, customers, or vendors to gain unauthorized access.

**Social Engineering Principles**

* **Effectiveness**: Exploits human trust and respect for authority.
* **Reasons for Effectiveness**:
  + **Authority**: Impersonates individuals with power to exploit conditioned respect for authority.
  + **Intimidation**: Uses bullying tactics to persuade and intimidate victims.
  + **Consensus/Social Proof**: Uses others’ trust to appear legitimate.
  + **Scarcity**: Implies limited supply of goods or services.
  + **Familiarity**: Establishes fake emotional connections to exploit users.
  + **Trust**: Develops emotional relationships to gain personal information.
  + **Urgency**: Persuades quick responses without questioning.

**Key Takeaways**

* **Understanding Attacks**: Familiarity with different attack methods helps in better protection.
* **Social Engineering**: Highly effective due to human nature and social behaviors.
* **Continuous Learning**: Ongoing opportunities to develop understanding and defense against cybersecurity attacks.

These notes should provide a comprehensive understanding of common attacks and their effectiveness in the cybersecurity landscape.