**IT Security - Phishing Presentation**

**1. Introduction**

* Definition of IT Security.
* Importance of protecting information.
* Types of cyber attacks.

**2. What is Phishing?**

* A deception method to obtain credentials.
* Cloning legitimate websites.
* Use of emails and malicious links.

**3. Attack Demonstration**

**Phase 1: Creating the Fake Page**

* Explanation of the HTML and PHP code used.
* How credentials are captured.

**Phase 2: Executing the Attack**

* The user enters credentials on the cloned page.
* Data is captured in datos.txt.
* Redirection to the real site.

**4. Attack Analysis**

* How cybercriminals deceive victims.
* Common mistakes users make.
* Impact of these attacks on businesses and individuals.

**5. Defense Methods**

**1. URL Verification**

* Checking if the domain is legitimate.
* Use of HTTPS and SSL certificates.

**2. Two-Factor Authentication (2FA)**

* Explanation of how 2FA prevents unauthorized access.
* Applications and implementation methods.

**3. Use of Password Managers**

* How password managers detect fake sites.
* Best practices for credential management.

**4. Education and Awareness**

* Cybersecurity training.
* Phishing simulations in organizations.

**6. Conclusion**

* Importance of IT security.
* Measures to avoid becoming a phishing victim.
* Final demonstration of best practices.

🎤 **Thank you for your attention! Questions and comments.**