**Don't Get Caught by Phishing Scams!!**

In today's digital age, we rely heavily on email and online communication. Unfortunately, this has created opportunities for cybercriminals to develop increasingly sophisticated methods have been developed to deceive us. One of the most common and dangerous is **phishing**.

**What is Phishing?**

Phishing is a cybercrime where attackers contact their victims by impersonating legitimate institutions such as banks, social networks, or government agencies. They typically request sensitive information like usernames, passwords, and credit card details, which they then use to steal identities or financial resources.

These deceptive messages are often very convincing, even using the same logos and language as real organizations.

**How to Spot a Phishing Attempt**

* **Suspicious links:** Be wary of links in emails, especially if they look unfamiliar or shortened.
* **Requests for personal information:** Sensitive information like passwords or bank details are rarely requested by legitimate organizations via email.
* **Unexpected emails:** Caution should be exercised when emails are received from organizations with whom interaction is not normal.

**Tips to Protect Yourself**

* **Strong passwords should be created** using a mix of upper- and lower-case letters, numbers, and symbols.
* **Two-factor authentication is recommended** for extra security. This adds an extra layer of protection, such as a code sent to your phone, in addition to your password.
* **Software should be kept updated.** Make sure your antivirus and anti-malware software are up to date.
* **Information should not be shared.** Be careful about sharing personal information online or via email.

**Stay Safe Online**

Phishing is a serious threat, but protection can be achieved through awareness and caution. Remember, your personal information is valuable.

Stay safe online Your security is in your hands!!!