Social Engineering

**Personalized Attacks**

With data breaches being so common now, it’s easy for cyber criminals to find or purchase large databases of personal information on millions of people. They then use this information to personalize their scams, making their emails, messages, or phone call attacks far more effective.

Criminals use these personal details to scare or pressure you into doing whatever they want. For example, a cyber attacker may collect your password when you visit a hacked website, and then use that information to trick or fool you into thinking they have hacked your computer.

Using personal information about you such as your full name, passwords you have used in the past, phone numbers, where you have worked, or other details that may have been found online.

Using emotions like fear, urgency, or embarrassment to try to rush you into making a mistake.

Demands for payment requiring methods such as Bitcoin or other crypto currencies.

It’s natural to feel scared when an attacker has personal information about you.

Knowing that emails or phone calls like these are a scam can make it easier for you to recognize them. Some of the most common indicators of a personalized attack are:

If you receive a suspicious email, stay calm; the more urgent the message, the more likely it is a scam. Try searching the internet to see if other people have reported similar attacks. In the end, common sense is your best defense.