Phishing scams are a common way of tricking individuals into giving out their personal information. By doing this, they intend to steal your account numbers, passwords or Social Security Numbers. Most of the times, the purpose behind phishing scams is to get organizational secrets or an individual’s financial information. The attackers can then misuse your account details or even conduct identity theft. Internet scammers use these phishing scams every day – and are often successful. Though these techniques keep on changing, there are some common signs that can help you recognize a phishing email or text.

**Recognizing Phishing Scams**

* A phishing email may look like it’s from a company or individual you trust or know. For instance, it may be from a bank you have an account with, a social networking site or an online store you often conduct transactions at.
* Phishing scams often try to put a bait for users by telling a story or background to make it sound very real. They may claim that your bank has detected several login attempts to your online account or noticed a suspicious activity. They may ask you to confirm some personal information or claim that your payment information is incorrect.
* Sometimes, they trick users by offering a reward that seems too good to be true. For example, winning a lottery you were never a part of, or free air tickets to Disneyland, etc.
* After creating a fake story or scenario, a phishing email or text will almost always ask you to click on a link or open an attachment.

At a first glance, the emails look perfectly authentic to the receiver. However, they are not. In fact, we all receive many such email in our spam inboxes every day. For a person who is new to the internet world and not very knowledgeable about online fraud, phishing scams can be a real threat.

**Avoiding Phishing Scams**

Apart from staying knowledgeable and learning how to identify phishing scams, it’s also important to take extra security measures.

It’s always a good idea to

* Use Multi-Factor authentication for your sensitive accounts. It adds an extra layer of security to your account by asking for extra credentials when logging in. It can be a fingerprint or an authentication code received via SMS or app. So even if a scammer gets your username and password, they will be unable to log into your account.
* Back up your data. Save your confidential data in cloud or an external hard drive. Also back up data on your phone.
* Keep all your systems up-to-date with latest security patches.

It’s also important for organizations to educate their employees and make security awareness a part of employee orientation. Doing this can prevent the chances of human error and save your organization from suffering a major data breach.