Bank account details: FBR warns taxpayers of fake emails

The Federal Board of Revenue (FBR) has strictly advised taxpayers and general public not to send their bank account details and passwords to any e-mail received from any e-mail address that is apparently from the FBR. According to an FBR announcement here on Tuesday, the FBR has directed taxpayers to be aware of fraudulent e-mails - phishing scams.

The FBR informed the taxpayers that the FBR does not send e-mail requesting taxpayers PIN numbers, passwords or similar access information for credit cards, banks or other financial accounts. The FBR said that there are numerous attempts by individuals and groups to solicit personal information from unsuspecting users by employing social engineering techniques. Various e-mails are crafted to appear as if they have been sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent website that appears legitimate. The user then may be asked to provide personal information such as account, usernames and passwords, which can further expose them to future compromises.

Additionally, these fraudulent websites may contain malicious code. E-mails designed to obtain taxpayer's banking information in lieu of facilitating a refund to the taxpayer or any other activity associated with an individual's bank account are extremely dangerous with an intent to defraud the individual. The FBR strictly advises the taxpayers from disclosing any information, especially related to their bank accounts via these e-mails and associated links.

This is called phishing and it is used by identity thieves around the world, who misuse the online financial systems and deprive unsuspecting people of their money. Globally, phishing deprives people of around US $ 1 billion annually.

The FBR further said that email phishing refers to the act of creating and sending fraudulent or spoofed e-mails with the goal of obtaining sensitive financial and personal information. Under such schemes, e-mails are designed to look exactly like the ones that are sent by legitimate companies. Sophisticated phishing attacks use the e-mail addresses of people who are registered to use certain services. When those people receive e-mails that are supposed to be from those companies or institutions, they are more likely to trust them. Spoofed e-mails often contain links that lead to spoofed websites, where various methods are used to request and collect a person's financial and personal information. Forms are occasionally contained within the e-mails themselves too.

The FBR cautioned the taxpayers that there are many signs of a phishing email. "The first thing that you should look at is the greeting. Does it use your actual name, or does it have a generic greeting? Look closely at the email's header. What is the sender's email address? These addresses are usually carefully designed to look authentic. By taking a very close look at them, though, you can usually see inconsistencies and things that don't make sense. If possible, compare the sender's email address to that of previous messages from the same company. If it's a phishing email, you will notice things that don't add up. The people often fall for these ruses because they are afraid of losing access to these important services. Both companies now offer extensive information on ways to avoid such phishing scams on their websites." There is no simple way to completely avoid e-mail phishing attacks. "Sooner or later, someone is bound to send you a spoofed email. The easiest way to avoid these scams is by never clicking on links that are included in email messages. Make it a policy to always type in the URL of the site that you need to access manually. Upon arriving on the site, you will be able to confirm whether or not the message that you received was legitimate. If it's a spoofed email, find out where to send it - most companies & institutions like to know about the scams that are going on out there."

The FBR said, "Once you believe you have come across a phishing Page you should immediately report the concerned page to Google via the following link: https:// safebrowsing.google.com/safebrowsing/report_phish/?hl=en"

This will help to ensure that unsuspecting visitors & users are warned before they are duped in divulging sensitive information compromising their financial accounts and associated information.