Beware of Fraudulent Emails - Phishing Scams

Disclaimer

- Federal Board of Revenue (FBR) does not send e-mail requesting Taxpayers PIN numbers, passwords or similar access information for credit cards, banks or other financial accounts.

Background

There are numerous attempts by individuals & groups to solicit personal information from unsuspecting users by employing social engineering techniques. Various emails 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. Emails 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. FBR strictly advises the taxpayer from disclosing any information especially related to your bank accounts via these emails 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 a billion US$ annually.

What is Email Phishing?

Email phishing refers to the act of creating and sending fraudulent or spoofed emails with the goal of obtaining sensitive financial and personal information. Under such schemes, emails are designed to look exactly like the ones that are sent by legitimate companies. Sophisticated phishing attacks use the email addresses of people who are registered to use certain services. When those people receive emails that are supposed to be from those companies or institutions, they are more likely to trust them. Spoofed emails 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 emails themselves too.

Signs of Email Phishing

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.
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 email 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.

Reporting Phishing Page

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. Furthermore, suspected links to Phishing pages can be reported to the National Response Center for Cyber Crime in order to flag & stop them from functioning from defraud unsuspecting individuals:

http://www.nr3c.gov.pk/creport.php

If you receive an e-mail or find a website you think is pretending to be of FBR, forward the e-mail or website URL to sec.website@fbr.gov.pk
You may forward the message as received or provide the Internet header of the e-mail. The Internet header has additional information to help us locate the sender.
After you forward the e-mail or header information to us, delete the message.

Sample Phishing Emails

- Click here to see reported Sample Phishing Emails
- Click here to see FBR's Public Awareness Press Releases on Phishing attackes.

Important Recommendations/Advisory

If you receive an e-mail from someone claiming to be the authorized by FBR or directing you to an Income Tax website:

- Do not reply.
- Do not open any attachments. Attachments may contain malicious code that will infect your computer.
- Do not click on any links. If you clicked on links in a suspicious e-mail or phishing website then do not enter confidential information like bank account, credit card details.
- Do not cut and paste the link from the message into your browsers, phishers can make link look like real, but it actually directs you to different websites.
- Use anti-virus software, anti-spyware, and a firewall and keep them updated. Some phishing e-mails contain software that can harm your computer or track your activities on the internet without your knowledge. Anti-virus & Anti-spyware software and firewall can protect you from inadvertently accepting such unwanted files.

The taxpayers and general public are advised not to send their bank account details and password to any emails received from any email address that is apparently from FBR. Any link to any bank is not provided on FBR's website and FBR would never ask for your bank details and passwords on its home page. Banks always advise their customers against disclosing their password even to bank officials or bank's genuine websites. Public is requested to be careful and prudent regarding such emails and the links provided through such emails. All taxpayers and general public are requested not to trust such emails and never disclose their bank account numbers, passwords and other details.

These precautionary instructions are being issued in the public interest and public is also advised that if someone has become a victim of this phishing attack through using the link sent through above mentioned email, they must immediately change the password of the relevant online bank and never share it with anyone .