RIVER BANK
We Bring Banking to You!

EMAIL PHISHING

Protect Yourself from Phishing Scams
Have you ever been manipulated into doing something you normally wouldn't do? Maybe you weren't aware of it at the time, and you realized you were duped after the fact. It's happened to most of us. Social engineering is all about manipulation. Phishing is a form of manipulation perpetuated over digital communications like email.

By sending out massive amounts of phishing emails, social engineers attempt to find a few gullible victims to get their hands on things like usernames, passwords and credit card details. They use email spoofing to masquerade as a trustworthy source in order to deceive people. In email spoofing, the email header is forged to make the message appear to come from someone or somewhere other than the actual source. They lure unsuspecting victims by making the email look as though it were sent from your bank, a popular social website, one of your personal friends, or just about any legitimate source.

The most common technique is to send an email to thousands of online users asking them to re-enter or update their personal information under the pretext that their "account is about to expire" or "multiple log-ins have been detected" or they've "just won the lottery." The message often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. The fake website either collects the confidential information you enter, or it is riddled with malware that will infect your computer or smartphone.

Once infected, these cybercriminals can steal your credentials by monitoring and intercepting your keystrokes or grabbing screen shots to steal your personal details and login credentials. Even worse, they can turn your computer into a robot to perpetuate their crimes, without you even knowing it.

Phishers are often very organized and connected. For example, they research social media profiles to gain intelligence about people they're targeting. Their goal is to build highly-personalized "lures" that are likely to be opened and acted upon. They may go after one piece of information, such as an ATM card PIN, to correlate it later with existing information, such as the card number and CVV. Once they obtain what they're looking for, they can quickly convert it into cash.

RIVER BANK
We Bring Banking to You!

How can I protect myself?
To help you spot an email phishing attack, ask yourself these questions:

1. **Who is the email from?** Is the sender's name or email address familiar to you? Does it use a webmail account like Hotmail when it claims to be from my bank?
2. **Is there a URL in the email?** Where's the hyperlink going to? When in doubt, don't click on it! As a best practice, always type the site address into the browser yourself (www.example.com) to ensure that the browser goes to the expected site.
3. **Is there a threat of immediate detrimental action** if you don't respond with personal information? A message demanding an immediate response deserves a good dose of skepticism.
4. **Does the email refer to a current news event?** Large-scale catastrophes or the death of celebrities are quickly followed by a wave of phishing messages touting the same news events in their subject lines or email body. Phishers are hoping that overeager users will let their guard down and click on the links in their haste for more information.
5. **Does the tone of the email from friends or colleagues sound right?** Filter the messages based on what you know of the purported sender(s) and how they typically write.

The single most important key to avoiding social engineering attacks is to not give sensitive information to anyone unless you can verify that they are who they claim to be, and that they have a legitimate need for access to the information.

MySECURITY Awareness.com

FDIC