RIVER BANK
We Bring Banking to You!

PHISHING

What is Phishing?

Cybercriminals are finding it more & more difficult to hack into systems, so they are choosing an easier target: PEOPLE!

- Phishing is an example of social engineering techniques used to deceive people into divulging information. Phishing is the fraudulent practice of sending emails purporting to be from legitimate companies in order to induce individuals to reveal personal information, such as usernames, passwords & credit card numbers.
- Phishing is a scam that uses official-looking email to lure individuals to a scam website in order to obtain their banking or credit card information for use in identity theft.
- The sender will typically steal the logo from a well-known bank or other authority and attempt to format the email to look legitimate. The email asks the user to click on a link leading to a fake and malicious website or to reply to the email with personal information.
- If you fall for the deception, the phisher will use the information you provide to steal your identity and your money.
- Legitimate companies do not send these requests to their customers.

Understand that no email communication is 100% secure, but we can do our best to bring the percentage close to that by following these guidelines:

1. **Protect your email address** – your email address is like your phone number and exposing your email address online puts you at risk of being targeted by cyber criminals and spammers – think twice before you use it or use a disposable address that you don’t use much, keep your real address private and only use it with your trusted contacts.
2. **Never reply to unsolicited emails** – even to complain. Acknowledging a spam email only validates your email address and can lead to more spam.
3. **Always avoid clicking on any hyperlinks** contained in an unsolicited email, or opening any kind of file attached to such a message as these can be disguised and often serve only to confirm your existence to spammers or install malware onto your computer. Shortened hyperlinks from URL shortening services are popular online, but are also abused by spammers and may redirect your browser to a malicious website.

4. **Avoid downloading pictures in spam emails** – these can be used to notify the spammer that the message has been opened. Many email applications allow you to turn off images except for those from trusted sources.
5. **Avoid scams and advance-fee fraud emails** – if it seems too good to be true, it probably is – the only way you can ever win a lottery is by taking part.
6. **Be careful how much information you share** about yourself on social networking sites and be careful who you add to your trusted circle of friends. Always make good use of the privacy controls on the social networking site in order to limit what others can see on your profile. It may take some time, but it is worth the effort.
7. **Treat with extreme caution any unsolicited email** arriving in your inbox that purports to be about a major current news story – it is likely to be spam.
8. **Don't use unsecure email accounts to send and receive sensitive information**.
9. **Don't send personal and financial information via email.** Banks and online stores provide, almost without exception, a secured section on their website where you can input your personal and financial information. They do this precisely because email, no matter how well protected, is more easily hacked than well-secured sites. Consequently, you should avoid writing to your bank via email and consider suspect any online store that requests you send them private information via email.
10. **Encrypt your important emails**. No matter how many steps you take to minimize the chance that your email is being monitored by hackers, you should always assume that someone else is watching whatever comes in and out of your computer. Given this assumption, it is important to encrypt your emails to make sure that if someone is monitoring your account, at least they can't understand what you're saying. Today, most reputable webmail service providers (Gmail, Hotmail, Yahoo!, etc.) offer free email encryption services.

Securing your email transmission is one step toward ensuring a safer and more enjoyable digital communication experience.