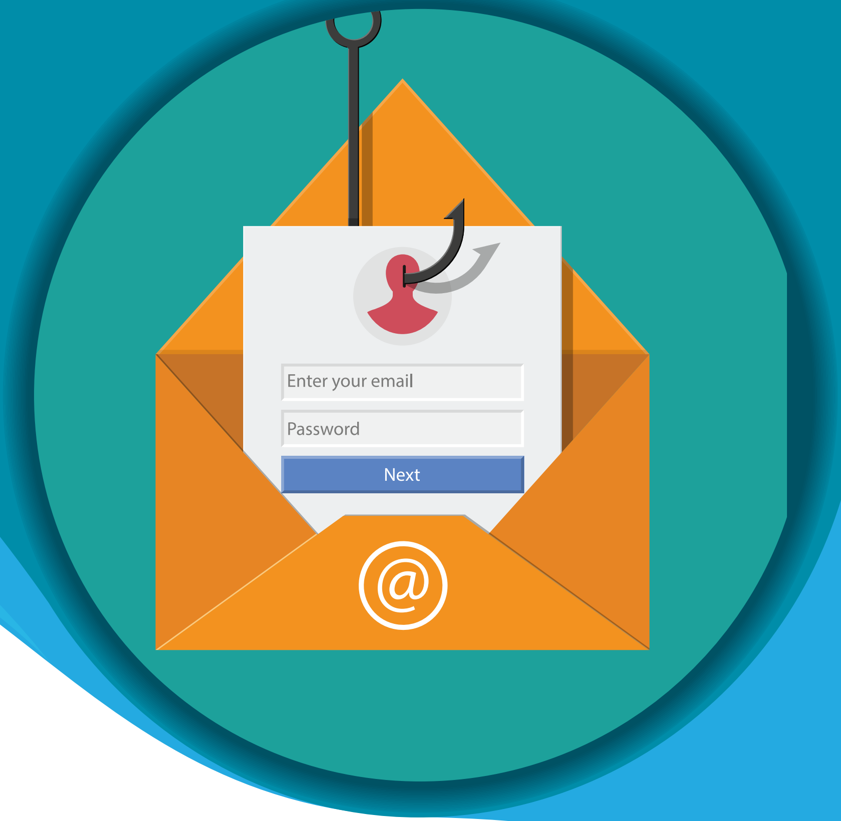
Do NOT get hooked!

Protect yourself against **Phishing.**
Be aware of this increasingly
destructive criminal activity.

GBTI

We see Guyana through your eyes



What is **PHISHING?**

"Phishing" (pronounced fishing) is an attempt by criminals to access your personal and confidential financial information, such as usernames, passwords, account numbers and credit card details by purporting to represent a reputable organization or person via an email platform.

This information is used to process transactions on your bank accounts, credit card accounts and in some cases steal your identity.

"Phishing" messages would either request the customer to provide their private/confidential information or threaten serious consequences if the customer does not login and take action immediately.

These emails would generally ask customers to click on a link/open an attachment to provide login information for the reactivation or authentication of their service. Clicking on this link/opening an attachment and entering your login details provides the fraudster with your username and password. The fraudster, having this information, can now login using the captured login details and process transactions on the customer's account if he/she has an online service with a bank.

How can I **protect myself?**

- Do not provide any personal information (i.e. login, account information, date of birth, credit card number, etc.) via email, phone or social media messages.
- Pay attention to the grammatical structure of the email. Watch out for poor spelling, generic language and poor sentence construction.
- If the email is sent from an unfamiliar source, ignore it.
- Always ensure that you are logged onto an established site for any legitimate service using the official site.
- Report impersonated or suspected emails to your service provider immediately.
- Check links in emails by hovering over the link without clicking on it to ensure the information displayed matches the link.

How can I keep my **Electronic Devices Safe?**

Install security software to protect your device and run regular scheduled updates and system scans to ensure the security of your devices.

- Phishing emails can be used to install malicious software on your devices to steal personal information.
- Anti-spam software can be used to reduce the amount of unwanted emails sent to your inbox.
- Trusted Anti-virus software should be installed to protect against viruses and malware.
- Install a firewall, which can help you protect your computer on the internet by blocking unauthorized connections.
- Always keep your operating system (Windows, MAC OS, Android, etc.) up-to-date by installing all security patches. Failure to do so may put your computer at higher risk of malware infections.
- Make sure your wireless connection at home is encrypted and password protected.

GBTI will never send emails, or make unsolicited calls requesting online passwords, access codes or other sensitive data from its Customers.

Customers must always ensure that they first log on to our website, https://www.gbtibank.com before proceeding to sign on to our Direct Banking Service.

- Protect your mobile and tablet devices. Make sure no one is reading information from your device's as they could pick up login credentials or password information. If you are connected to public Wi-Fi, do not perform banking activities online. Also, do not store your passwords within your device, such as notes app.
- Do not respond to emails from companies or people you do not have a relationship with. If you receive a message asking you to urgently respond to an email or click on a link, check with the company before you respond to it.
- Do not click on links or open attachments from unknown sources, such as PDFs or ZIP files.

How can I keep my **Electronic Devices Safe?**

- Do not reply to any email that asks you to verify your account, reset your password or request confidential information.
- Do not enter your personal or credit information into a form that is embedded or linked to an email. If you think the email is legitimate, call the company or visit their website and log in securely before you enter the requested information. Always make sure the website address begins with “https” instead of “http” to protect your personal information while it is in transit.

GBTI

We see Guyana through your eyes