At Fortis Private Bank, we care deeply about cyber security and strive to provide you, our clients, with the knowledge, systems, and tools to help minimize the likelihood and impact of a cyberattack on your financial assets.

Fortis Private Bank's online banking systems bring together a combination of state of the art industry proven security technologies to protect data for the bank and for you, our customer. The bank monitors and works to enhance security to ensure the integrity of our online banking system. Our goal is to protect the confidentiality of your account and personal data, and to comply with all applicable banking regulations related to the safeguarding of your data.

Cybersecurity Awareness:

Online fraud and scams are prevalent in every industry and are increasing at alarming rates. Stay informed on the latest scams and tricks so that they won't catch you off guard.

Here are some proactive tips for keeping your bank account safe:

- Don't leave personal items like your wallet or purse in your car.
- Don't leave outgoing mail in your mailbox with the flag up. It is a notice to thieves that you may have checks in your mailbox.
- Don't write down PIN's or logins. Memorize them.
- Put a password on your account that only you know.
- Use caution with public unsecured Wi-Fi. Criminals may be waiting to access your device.
- Notify your bank as soon as you think your identity may have been compromised.

Protecting your personal information is a shared responsibility. Here are some proactive tips for keeping your personal information safe:

- When sending sensitive information via the Internet, make sure 'https:' appears in the address bar. This means the information you are transmitting is encrypted.
- Ensure the wireless network you use is password protected and choose a strong password and update it frequently for your work and home wireless networks. Likewise, always use a passcode on your mobile phone or tablet to stop an unauthorized user from accessing your device.
- Don't enter sensitive information into your phone when others can see what you're entering.
- Set the privacy settings on frequented social network sites. Cybercriminals often learn about people and their families and friends via social media in an attempt to spoof or phish you and your network.
- Remain cautious of someone who isn't who they say they are or if the name and area don't match what appears on caller ID. This is often how spoofing occurs.
- Never respond to text messages, emails or phone calls from companies alleging to be your bank, government officials or business representatives that request your banking ID, account numbers, user name or password.

- Similarly, don't click on links sent to you from unknown sources via text message because they are likely malware.
- Beware of 'get rich quick' schemes; never voluntarily give out your bank account information or security credentials.

Here are some protective tips for keeping your personal data safe on your mobile phone:

- Always lock your phone when not in use.
- Set up Finger-Print or Facial Recognition (if available).
- Don't download apps from third-party sites.
- Always back up your smartphone's data. Your Phone's Service Provider may already offer a plan.
- Keep your phone's Operating System (OS) updated.
- If your phone is lost or stolen, contact your Service Provider immediately.

Protecting Yourself Against Email Fraud:

Internet "phishing" scams are one of the fastest-growing frauds today. Phishing typically involves a phony email message that uses legitimate materials, such as a company's website graphics and logos, in an attempt to entice email recipients to provide personal financial details, such as credit card and Social Security numbers.

Fortis Private Bank will NEVER request personal financial information via email. To reach our website, always type in our website address, https://www.fortisprivatebank.com.

Here's how you can guard against this form of fraud and help fight back:

Stop, Look and Call:

The Department of Justice advises e-mail users to "stop, look and call" if they receive a suspicious email.

- Stop – Do not immediately respond to a suspicious email.
- Look – Read the text of the email several times and question why the information requested would be needed.
- Call - Telephone the organization identified, using a number you know to be legitimate.

If you receive a suspicious email that appears to be from Fortis Private Bank, please report it immediately by forwarding the email to info@fortispb.com. Never respond to an unsolicited e-mail that is requesting financial information.

If You Have Been "Phished"

If you think you have provided financial information about yourself through a phishing scam, you should:

- Contact your financial institution

- Contact the three major credit bureaus and request that a fraud alert be placed on your credit report. The credit bureaus and phone numbers are as follows:
    - Equifax 1-800-525-6285
    - Experian 1-888-397-3742
    - TransUnion 1-800-680-7289
- File a complaint with the Federal Trade Commission or call 1-877-382-4357.
- If you think you have received a phishing email or have been directed to a phishing website, you can also contact the Internet Crime Complaint Center (IC3), which is a partnership between the FBI and the National White Collar Crime Center.

Other Security Concerns:

If you experience any type of fraudulent activity related to your account or online banking, please contact Fortis Private Bank immediately at 720-616-4000.

Additional Resources:

If you are interested in learning more about how you can protect your personal data, additional resources are available:

Internet Crime Complaint Center (IC3)

Identity Theft