KISH BANK | Security Tips

Online/Mobile Safety Tips

General Guidelines

- Use security and privacy settings on social network sites, and beware of random contact from strangers.
- Be wary of phone or email requests to update or verify personal information.
- Research apps before downloading, and download only from an app store (iTunes, Play Store, Windows Store). Do not assume an app is safe because the icon resembles that of a bank.
- Enroll in digital banking account alerts for your Kish Bank account so that you can monitor your account activity at all times.
- Install some form of Anti-Virus, Anti-Malware, or Anti-Spyware protection on every device. There is a variety of software available for free.

Email Safety

- Do not click on links in emails or open attachments unless the email was expected/verified; confirm a message is legitimate by contacting the sender directly via pre-determined contact information.
- Be on guard against fraudulent checks, cashier's checks, money orders, or electronic fund transfers with a request to return part of the funds via wire transfer.
- Beware of disaster-related scams, where scammers claim to be from legitimate charitable organizations.
- **The Red Flags:**
  - » The sender is someone you do not recognize.
  - » The content is unusual or out of context for a recognized sender.
  - » The message contains general salutations and/or signatures.
  - » The sender is asking for personal information.
  - » There are misspellings and/or typos in either the content or the hyperlinks.
  - » The message asks you to take fast action, offers something that sounds too good to be true, or instills a sense of fear.
  - » The email includes attachment(s) whose names do not seem to match the content.
  - » Actual URLs differ from the link text in the email.

Password Protections

- Create long passwords with at least 10 characters, using a mix of alpha-numeric characters (A, b, 1, 99) and symbols (@, $, %, *).
- Instead of a password, use a passphrase: a long (15-25 character) phrase or sentence that only makes sense to you and is easy for you to remember. Do not use something common like "Maryhadalittlelamb"; instead, use something uncommon like "MichaelWhassocceronThursdays."
- Use a password checker to verify the strength of the selected password. Do NOT put a valid password into an online password checker; instead, use a variation that is similar but not the same.
- Do not use the same password for two critical websites or online accounts, do not share passwords with others, and do not use the "Remember My Password" feature in web browsers.
- Unless you use a very long and difficult password, change passwords often.
- Use a password manager to enable longer passwords without having to write them down.

Source: American Bankers Association

Member FDIC 05/2020