Fraud Tips

Prevent Fraud Before it Happens

Preventing fraud is much easier than recovering from it. Here are some best practices to help protect you.

Preventing Fraud

1. **Only share information on a 'need to know' basis.** The fewer people with whom you share information, the less likely you will fall victim to identity fraud. It is important to only disclose the information if necessary, and only if you trust the recipient of that information.
2. **Do not assume an email or call is authentic.** Just because someone knows your basic information (such as your name, date of birth, and address), it doesn't guarantee the email or phone call is legitimate.
3. **Get your free credit report.** Each year you may receive 1 free credit report from each of the 3 credit reporting agencies (Trans Union, Equifax, or Experian). Once received, check for unauthorized accounts, inquiries, and unknown addresses.
4. **Know your recipient.** When making person to person payments, (i.e., Zelle, Venmo, etc.), pay and receive money *only* with people you know personally.
5. **Do not pay for merchandise online or via the phone using a debit card.** Debit cards are vulnerable because they are linked to a bank account. You have a far better chance of resolving a fraudulent transaction when paying with a credit card than with a debit card.

Do not wait until you become the victim of a fraudster. The time and effort to protect yourself can save you substantial inconvenience and money. For more information on protecting your finances, visit our website or contact your local HBC branch.

Implementing Online Security

1. **Set up two-factor authentication on any account that allows it.** This will alert you, typically via text or phone call, whenever someone is attempting to log into one of your accounts or applications.
2. **Think before clicking or downloading.** Don't click on anything in an unsolicited email, text, social media, or messaging application. Validate any message asking you to update or verify account information by calling a known number for that business. Never open an email attachment from someone you don't know, and be wary of email attachments forwarded to you, even if you know the person forwarding it.
3. **Verify email addresses.** Carefully examine the email address, URL address, and spelling used in any emails or text messages. Scammers use slight differences to trick your eye and gain your trust. Watch for grammatical and spelling errors in the message as these can be common in fraud attempts.
4. **Use strong passwords and change them regularly.** Do not use common words or names, and add unusual characters to make the password difficult to guess.
5. **Protect your sensitive personal information.** Scammers often use personal or common information, such as pet names, schools you attended, links to family members, and your birthday, to send phishing emails, guess your password, or answer your security questions. Be cautious about providing this type of personal information in social media (such as through "contests" or "surveys") as this is one method used by fraudsters to gather non-public details.

HERITAGE
BANK OF COMMERCE

www.HeritageBankofCommerce.bank