Fraud Tips for Business Owners

Preventing fraud and cybersecurity attacks is much easier than recovering from them. Here are some best practices to help stop these breaches from impacting you and your business.

Business

Preventing Fraud

1. **Ensure you establish an environment of compliance within your organization.** Set a tone of honesty and integrity with your staff, encouraging adherence to rules and procedures at all levels. Foster an environment that will allow staff to report mistakes to ensure prompt resolution and prevention of future errors.
2. **Establish dual control processes for any tasks that involve money.** This requires two staff members that have the authority to approve transactions. Set system authorizations and authorities at a level that allows staff to complete their responsibilities, but does not allow access above what is needed.
3. **Be vigilant.** Conduct due diligence on all business associates and third parties. Watch out for red flags of suspected fraud, including indications of employee fraud, vendor fraud, customer fraud, or cybercrime.
4. **Ensure anti-virus software is up to date.** Ensure updates are installed as soon as they become available to address known vulnerabilities. Promptly contact technical support at the first sign of potential cyber fraud or email/system intrusion. Conduct ongoing training of staff on security to prevent malware. (See "Implementing Cybersecurity" section.)
5. **Contact your bank immediately upon detection of fraud.** Your bank can support recovery efforts and provide guidance on additional fraud prevention tools.

Implementing Cybersecurity

1. **Train employees in security principles.** Establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet-use guidelines that detail penalties for violating company cybersecurity policies.
2. **Passwords and authentication.** Require employees to use unique passwords and change passwords frequently. Consider implementing multifactor authentication that requires additional information beyond a password to gain entry.
3. **Secure your Wi-Fi networks.** If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, and hidden. Password protect access to the router.
4. **Provide firewall security for your Internet connection.** A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.
5. **Conduct a security risk asessment.** Understand the most critical threats to your business and conduct regular security assessments, particularly for those that must adhere to compliance standards and regulations.

HERITAGE
BANK OF COMMERCE

www.HeritageBankofCommerce.bank

Fraud Tips for Business Owners

Personal

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 and your business can save you substantial inconvenience and money. For more information on protecting your finances, visit our website or contact your local HBC branch.

Implementing Cybersecurity

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