CITIZENS BUSINESS BANK

cbbank.com/security

CYBERSECURITY

Most of us hear about cyberfraud in the news but never believe we could be misled by a fraudster. The truth is cyberfraud is so lucrative that even organized crime has started targeting businesses. Believing you or your employees will not fall for these sophisticated scams is a risk you should not take. It only takes one email and a few minutes to become exposed to cybersecurity risks.

COMMON PRACTICES TO FOLLOW

Always verify any email requesting the wire transfer of funds, even when it comes from a known source. Pay particular attention to beneficiary name and account number.

Always be suspicious of unsolicited emails, even from a known source.

Never click on attachment links in unsolicited or unusual emails.

Never rely solely on a fax or email request to wire funds or purchase/ship goods.

Never respond to unsolicited phone calls, emails, or text messages requesting sensitive information.

Note: The IRS, FDIC, Better Business Bureau, NACHA, and others never use email to deliver requests to resolve issues regarding penalties, infractions or complaints, and you should be suspicious of any such request. In addition, Citizens Business Bank will never ask you for your password or other security codes via text, email, or popup message.

SAFETY PROCEDURES TO FOLLOW

Develop a **review process** for handling every incoming email/fax demand for payment, especially for requests to change wire transfer instructions, customize orders, or unusual vendor requests.

Implement a **strong password** policy for all devices, system applications, and network access points.

Implement **dual authorization** and separation of duties for monetary processes.

Implement controls to **restrict website access**.

Regularly review computer, network, and internet security policies and procedures with staff.

Dedicate a computer for online banking activity and no other internet use, particularly when initiating wire transfers and originating ACH transactions.

Reconcile bank accounts **daily**.

Develop **internal cybersecurity procedures**.

Maintain up-to-date anti-virus, anti-malware, and anti-spyware software.

Limit the number of staff with **administrative rights** on your computers.

Restrict and monitor the installation of unauthorized software.

Secure firewalls, routers, and wireless devices connected to your network.

Use **encryption** to protect sensitive data.

If you suspect your personal information, your company information, or your network has been compromised, please contact us at 888.228.2265 immediately. You may also want to contact the appropriate authorities and immediately perform a computer/network security assessment or hire a reputable third party to assess your computer and Internet environment.