PRIME MERIDIAN BANK™

Cybersecurity Threats and Best Practices

Prime Meridian Bank recognizes the growing risks and exposures of cyber threats. While we encourage you to seek advice from industry experts, we have compiled an overview of a few common risks and recommendations for protection.

BUSINESS EMAIL COMPROMISE (BEC)

Business email compromise (alternately, email account compromise) exploits the reliance on email to conduct business. Generally, a criminal sends an email to request money. These requests can be from fraudulent sources that appear legitimate or from legitimate business partners whose email has been hacked or otherwise compromised by a criminal. The best prevention is to always verify any payment change requests by phone at a number that was obtained prior to the email. Any information contained in the email should be scrutinized and verified out-of-band. More information can be found at:

http://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

WEBSITE SPOOFING

Website spoofing is the act of creating a fake website to mislead individuals into sharing sensitive information. Spoofed websites are typically made to look exactly like a legitimate website published by a trusted organization.

Prevention Tips:

- Pay attention to the web address (URL) of websites. A website may look legitimate, but the URL may have a variation in spelling or use a different domain.
- If you are suspicious of a website, close it and contact the company directly.
- Do not click links on social networking sites, pop-up windows, or non-trusted websites. Links can take you to a different website than their labels indicate. Typing an address in your browser is a safer alternative.
- Only give sensitive information to websites using a secure connection. Verify the web address begins with "https://" (the "s" is for secure) rather than just http://.
- Avoid using websites when your browser displays certificate errors or warnings.
- Be careful when selecting Google results because the top results typically are ads. A person spoofing a website may purchase ad space to have their results at the top.

PHISHING

Phishing is when an attacker attempts to acquire information by masquerading as a trustworthy entity in an electronic communication. Phishing messages often direct the recipient to a spoof website. Phishing attacks are typically carried out through email, instant messaging, telephone calls, and text messages (SMS).

Prevention Tips:

- Delete email and text messages that ask you to confirm or provide sensitive information. Legitimate companies don't ask for sensitive information through email or text messages.
- Beware of visiting website addresses sent to you in an unsolicited message.
- Even if you feel the message is legitimate, type web addresses into your browser or use bookmarks instead of clicking links contained in messages.
- Try to independently verify any details given in the message directly with the company.
- Utilize anti-phishing features available in your email and/or web browser.
- Do not click on links in text messages that you are NOT expecting. If you receive a text, avoid clicking on any links—instead, go directly to the applicable website (e.g. from Amazon, USPS, FedEx, etc.).

TYPOSQUATTING

Typosquatting, also known as URL Hijacking, occurs when a website contains a slightly different spelling in the URL (e.g. "Gooogle.com" instead of "Google.com"). The fake website often appears very similar to the intended website, and aims to steal personal identifiable information. The best way to counter typosquatting is to slow down and read the domain of URLs carefully.

FRAUD PREVENTION SERVICES

Prime Meridian Bank offers Fraud Prevention Services that may be a beneficial addition to your Online Banking services.

Secure Tokens:

- When implemented, Online Banking users are required to input a unique code generated by the Secure Token upon each log in to Online Banking.
- Three types of Secure Tokens available: Virtual App-based, Virtual Desktop-based, and Fob

Positive Pay:

- Positive Pay helps protect companies from having unauthorized or altered checks from clearing the bank account.
- The program matches the serial number and dollar amount of checks that are presented for payment against checks that were previously authorized and issued by the business.
- Items that do not match are flagged, and the business determines if the checks be paid or returned.

ACH Fraud Filters:

- ACH Fraud Filters monitors ACH debits and credits that attempt to clear the bank account.
- Filters are established for authorized ACH Originators.
- Incoming ACH transactions that do not have a filter established are flagged and reported to you for payment decision.

OTHER PREVENTION TIPS

- Be diligent in reviewing account activity at the start of each business day and report unauthorized, suspicious, or erroneous transactions to the bank immediately. Please be reminded, the bank must return any such items (checks or ACH transactions) within 24 hours of the transaction posting to your account in order to comply with regulations and ensure recovery of your funds.
- Do not share passwords or secure tokens. Consider changing passwords periodically.
- Ensure your computer is protected from unauthorized access by use of an anti-virus protection software.
- Protect the confidentiality and integrity of protected information until its destruction. Some examples of protected information include customer authorizations, social security number, account number and routing number information, policy numbers, etc.
- Protect sensitive information no matter what form it is stored as, e.g., electronically or paper based, from the point it is collected until it is destroyed. Restrict and limit access to sensitive date. Use locks on doors and file cabinets. Limit employee access to data to those that need it to do their jobs.
- Do not store sensitive information on portable storage devices (e.g., PDA's, USB drives, CDs, laptops, iPhones, iPods, etc.) as these devices are frequently lost or stolen. If sensitive information is stored on a portable device, ensure the device is encrypted.
- Consider obtaining a comprehensive Cybersecurity Insurance Policy to cover privacy, data, and network exposures commensurate with the type, volume and complexity of the data and business operations.