Cyber Security Awareness

TIPS AND TOOLS TO KEEP YOUR ACCOUNT SECURE

Home HB Bank

Safeguard your Systems and Data

Computer-related crimes affecting businesses and consumers are frequently in the news. This guide, developed by the Federal Deposit Insurance Corporation, provides cyber security information for financial institutions' business customers on how to safeguard computer systems and data.

PROTECT COMPUTERS AND NETWORKS

Install security and antivirus software that protects against malware, or malicious software, which can access a computer system without the owner's consent for a variety of uses, including theft of information. Other protections include firewalls, keeping software current, encrypting wireless networks and using strong passwords.

REQUIRE STRONG AUTHENTICATION

Ensure that employees and other users connecting to your network use strong user IDs and passwords for computers, mobile devices and online accounts by using combinations of upper-and lower-case letters, numbers and symbols that are hard to guess and are changed regularly. Consider implementing multifactor authentication that requires additional information beyond a password to gain access.

⚠ DON'T FORGET ABOUT MOBILE PHONES

Mobile devices can be a source of security challenges, especially if they hold confidential information or can access your business's network. If your employees connect their devices to the business's network, require them to password protect their devices, encrypt their data and install security apps to prevent criminals from accessing the device while it is connected to public networks. Be sure to develop and enforce reporting procedures for lost or stolen equipment.

Monitoring your accounts

Watch for unauthorized withdrawals.

In recent years, there has been an increase in unauthorized electronic transfers made from bank accounts held by businesses.

While Home Bank is required to have a vigorous information security program to safeguard financial data, business customers also need to know how to steer clear of fraudsters.

Put in additional controls, such as dual authorization for external financial transfers, as well as confirmation calls before financial transfers are authorized with the financial institution.

A common scam is an account takeover where cyber criminals use malicious software, such as keystroke loggers, to obtain the IDs and passwords for online bank accounts and then make withdrawals.

Another scam called Business Email Compromise, targets businesses forging payment requests for legitimate vendors and directing the funds to the cyber criminal's account.

Businesses are generally not covered by federal consumer protections against unauthorized electronic funds transfers. Therefore, Home Bank may not be responsible for reimbursing losses associated with theft if negligence on the part of your business, such as unsecured computers or falling for common scams, were factors in the loss.

Proactive Safety Steps

Stop cyber crime before it happens.

Control access to data and computers
Limit use of business computers to authorized employees. Have separate user accounts for each employee.

Teach employees the basics
Ensure all employees know how to identify and report potential security incidents.

Patch software in a timely manner
Download and install software updates as soon as they are available or set up for automatic downloads of updated software.

Make backup copies of important data
Regularly back up data from computers used by your business using encrypted storage methods.

Watch out for fraudulent transactions
Scams can range from payments with checks to debit cards. Be sure you have insurance to protect against risks and report any irregularities immediately.

Educate yourself
Learn more online at Home24Bank.com