FIRST COLUMBIA BANK & TRUST CO.

Protecting Your Business – Information Security Recommendations

Especially during these uncertain economic times, it may seem like the biggest risks to your business are revenue-related. (Can you stay open? Will customers come in? Will customers spend enough for you to make a profit? Are any of your suppliers affected by the pandemic?)

However, fraudsters and hackers have been taking advantage of the crisis, working overtime with new schemes to take what they can. Here are some suggestions to protect yourself and prevent cyber-frauds from affecting your bottom line.

1. **Insist that employees keep online banking login information secret and secure**.
   This means that they don't keep usernames and passwords on a post-it under the keyboard. They don't share their credentials with coworkers. When employees leave, their access should be immediately locked. Contact the bank to remove the access and for help with adding new employees with their own login credentials.

2. **Remind employees never to click on links or open attachments received via unsolicited email**.
   These links and attachments can load malware onto your computer and network. The malware can capture everything that is typed, copy confidential data that is then made public or sold, or hold your system for ransom.

3. **Load software patches and keep Anti-Virus Software up to date**.
   Windows 7 is no longer supported by Microsoft. This means that, unless you have a private agreement with Microsoft to continue providing patches, your computer running Windows 7 is vulnerable to hacking.

   Up to date anti-virus software is a simple way to defend against identified computer viruses. You can purchase a bundled software that includes anti-spyware, anti-malware, and anti-adware. The software companies are constantly adding new malware to their registry so that it can be identified on your computer when you run a scan.

4. **Only use a secure computer system with a firewall to access your online banking information**.

5. **Be aware of some of the common signs that your computer system may be compromised**.
   - Your computer runs more slowly than normal
   - A frequently-visited website looks different
   - The employee receives pop-up notices that the bank's website is down when trying to log into online banking
   - The computer locks up or cannot be shut down or restarted
   - Pop-ups requesting login information appear while you are already logged into online banking or using unrelated software
   - Contacts from your email program reporting receiving strange emails that appear to be coming from you