TechTip Postcard

Insider Tips and Secrets to Get The MOST Out of Your Computer APRIL 2013 — VOL 10 — ISSUE 4

The Single Most Dangerous Assumption Businesses Make About Bank Security That Can Cause Them To Lose ALL Their Money

Here's a shocker to most business owners: Your bank often can NOT reclaim money stolen from your bank account due to fraud or cyber-crime. That means if money gets drafted from your business bank account from a hacker, phishing attack, identity theft or by any other means, you have little to no chance of getting it back.

This often comes as a surprise to businesses who think the FDIC will "save" them from getting their accounts wiped out, and can get the money back once taken. The reality is that the FDIC insurance is to protect you from bank failure, NOT fraud. So if your debit card or account information gets accessed by a hacker and you don't notice it within the same day, you can pretty much kiss that money goodbye.

Recent studies have shown that 83% of small businesses take no formal measures against cyberthreats even though almost half of all attacks are aimed at them.

Here are 5 essential steps you can take right now to protect your business:

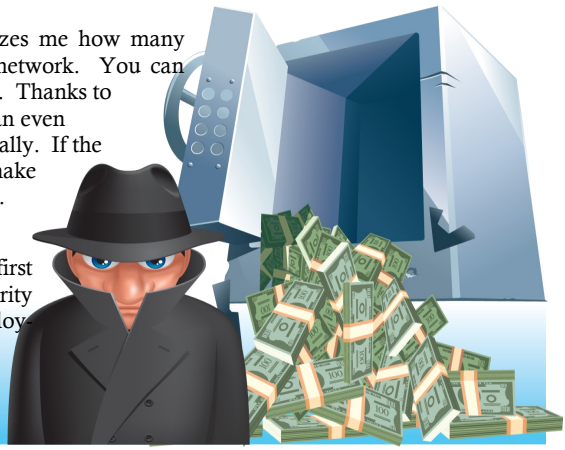
1. **Enforce A Strict Company Password Policy.** This is a simple step, but it is still violated by many companies every day. Make sure that you and your employees change passwords regularly, don't use the same password for all accounts and require complex passwords.

2. **Set Up A Firewall.** Small business owners tend to think that because they are "just a small business", no one would waste time trying to hack into their network. The fact is that hackers will target the weakest link. Without a firewall, that "weak link" is YOUR company.

3. **Designate A Banking-Only Computer. Banking fraud is one of the biggest threats to small business.** The 2011 Business Banking Study showed that 56% of businesses experienced payment fraud (or an attempt at fraud) and 75% experienced account takeover and fraud online. By using a single computer solely dedicated to online financial transactions (no e-mail, web-surfing, Facebook, YouTube, etc.) it's much harder for outsiders to gain access to your information.

4. **Back Up Your Files Daily.** It just amazes me how many businesses never back up their computer network. You can lose data as well as money in a cyber attack. Thanks to many new cloud based technologies, you can even schedule offsite backups to occur automatically. If the data in your business is important to you, make sure that you have more than one copy of it.

5. **Educate Employees.** You staff is the first line of defense AND your biggest security hole at the same time. Uneducated employees are one of the most common causes of data breaches. Make sure that they are aware of the do's and don'ts for your company with regards to data security.



JB TECHNOLOGIES
jbtech.com

John Kistler, President

180 Weldon Parkway
Maryland Heights, MO 63043

Download This Free Executive Guide Today! "What Every Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems"

Why Choose Our Company For Your Next IT Service:

- 100% Satisfaction Guarantee
- Rapid Response Within 60-Minutes or Less
- Reliable, Friendly, Knowledgeable Technicians
- Availability To Answer Your Questions
- "No Geek Speak"
- All Projects Completed On Time and On Budget – Guaranteed

This FREE Report Reveals What EVERY Business Owner Should Know About:

- Keeping your network safe from viruses, hackers, spam, spyware and other cyberthreats.
- Critical security measures to protect against natural disasters, major system failures, theft and corruption of sensitive data, and even employee sabotage.
- How to dramatically lower or eliminate expensive computer repair bills.
- How to get (and keep) your network running lightening fast.

To download this Free Report, call us now! 314-993-5528 Or go online to:

www.fixedforever.com/cyberthreats