First United®
SPEND LIFE WISELY®

Corporate Account Takeover

Protect Your Business From Corporate Account Takeover

What would you do if you suddenly noticed that large amounts of money had been drained from your business account?

Unfortunately, online criminals are using increasingly sophisticated techniques to commit payments fraud against commercial business accounts.

What is Corporate Account Takeover?

Corporate account takeover is a type of fraud where thieves gain access to a business' finances to make unauthorized transactions, including transferring funds from the company, creating and adding new fake employees to payroll, and stealing sensitive customer information that may not be recoverable.

Consider These tips to Ensure Your Business is Well Prepared

- Develop a security plan. Each business should evaluate its Corporate Account Takeover risk profile and develop a security plan that includes sound business practices.
- Protect your online environment. Use appropriate tools to prevent and deter unauthorized access to your network and make sure you keep them up to date. Encrypt sensitive data and use complex passwords and change them regularly.
- Create a secure financial environment. Dedicate one computer exclusively for online banking. This computer should not be connected to the business network, have email capability, or connect to the Internet for any purpose other than online banking.
- Partner with First United Bank to prevent unauthorized transactions. Talk to the Treasury Management Department about services that protect you from unauthorized transactions. Positive Pay can help protect your accounts from losses due to check fraud. Implementing security procedures such as call backs, device authentication, multi-person approval processes, alerts, and batch limits help protect you from fraud.
- Pay attention to suspicious activity and react quickly. Watch for unexplained account or network activity, pop ups, and suspicious emails.
- Educate all employees about cybercrimes. This will help them understand that even one infected computer can lead to an account takeover. All employees, even those with no financial responsibilities, should be educated about these threats.

Understanding Your Hard Drive

Computers often hold personal and financial information, including;

- passwords
- account numbers
- license keys or registration numbers for software programs
- addresses and phone numbers
- medical and prescription information
- tax returns
- files created automatically by browsers and operating systems

When you save a file, especially a large one, it is scattered around the hard drive in bits and pieces. When you open a file, the hard drive gathers the bits and pieces and reconstructs them.

When you delete a file, the links to reconstruct the file disappear. But the bits and pieces of the deleted file stay on your computer until they're overwritten, and they can be retrieved with a data recovery program. To remove data from a hard drive permanently, the hard drive needs to be wiped clean.

Tips on How to Clean a Hard Drive

Before you clean a hard drive, save the files you want to keep to another device such as an USB, or external hard drive.

Utility programs to wipe a hard drive are available both online and in stores where computers are sold. These programs generally are inexpensive; some are available on the internet for free. These programs vary:

- Some erase the entire disk, while others allow you to select files or folders to erase.
- Some overwrite or wipe the hard drive many times, while others overwrite it only once.

Consider using a program that overwrites or wipes the hard drive many times; otherwise, the deleted information could be retrieved. Or remove the hard drive, and physically destroy it.

Mobile Device Security

Follow these tips to protect your mobile device, data and privacy against the growing mobile malware threats.

1. Do not circumvent or disengage security features such as passcodes and auto-locks.
2. Set the device to lock after a set period of inactivity. A recommended inactive period setting is 10 minutes or less.
3. Ensure that you have GPS device location in the event of theft or loss.
4. Use caution when downloading apps and free software, especially from unsanctioned online stores.
5. Install an on-device personal firewall to protect mobile device interfaces from direct attack.
6. Install anti-spam software to protect against unwanted voice and SMS or MMS communications.
7. Install real-time anti-malware technology via cloud services that continually analyzes and re-analyzes websites and mobile applications. Protect against malicious applications, spyware, infected secure digital (SD) cards and malware-based attacks.
8. Turn off "beaming" (infrared data transmission).
9. Turn off the Wi-Fi when you're not using it; and avoid using public, unsecured Wi-Fi hotspots.
10. Before discarding any device, make sure it is wiped clean and restored to factory defaults.

Unfortunately, there is no straightforward, one-size-fits-all remedy to the mobile security problem, but there are definite steps you can take to protect your device and ultimately, your personal information.

Treasury Management

treasurymangement@firstunitedbank.com

580-634-6116