

Simmesport State Bank

Corporate Account Takeover

WHAT IS CORPORATE ACCOUNT TAKEOVER?

Corporate identity theft.

Simply put, corporate account takeover is the business equivalent of personal identity theft. Hackers, backed by professional criminal organizations, are targeting small and medium businesses to obtain access to their web banking credentials or remove control of their computers. These backers will then drain the deposit and credit lines of the compromised bank accounts, funneling the funds through mules that quickly redirect the monies overseas into backers' accounts. A computer can be compromised very easily by visiting an infected website or by simply opening an email. There has been a steady increase in account takeovers since 2009 resulting in billions of dollars of damage.

SECURITY BEST PRACTICES

A solid foundation to build on.

When it comes to protecting sensitive financial information from hackers, there's no substitute for good old-fashioned knowledge. As a business owner, you should have a level of understanding about how to secure your computers that allows you to take proactive steps and avoid, or at least minimize most threats. Experts advise following best practices including using a dedicated computer, keeping patches and anti-virus up to date, installing a host based firewall, verifying all transactions before approving and reviewing bank transactions daily. These best practices should be the minimum security baseline for every company's online banking transactions.

STEPS FOR BETTER SECURITY

- Use a **dedicated computer** for financial transactional activity. Do not use this computer for general web browsing and email.
- Apply **operating system and application updates** regularly (patches).
- Ensure that **anti-virus/spyware** software is installed, functional and is updated with the most current version.
- Have **host-based firewall** software installed on computers.
- Use the **latest version of internet browsers**, such as Explorer, Firefox or Google Chrome and keep patch up to date.
- Activate a "**pop-up**" blocker on internet browsers to prevent intrusions.
- **Turn off your computer** when not in use.
- **Do not batch approve transactions**; be sure to review and approve each one individually.
- Review your **credit report/banking transactions** regularly.
- Contact your information technology provider to determine the best way to safeguard the security of your computers and networks.