



malware and bank fraud

What It Is And How It's Done

Malware, or hostile software, can have serious adverse effects on a business. Through malware, fraudsters have the ability to take control of your computer or monitor your activity without your knowledge - meaning they can potentially steal sensitive information and even money out of your pocket. It occurs - or infects - when a company's employees either open a fraudulent or SPAM email, browse an infected website, download files via peer-to-peer file sharing, or "catch it" from other infected computers within the company's internal network. Here are more facts about how it happens and how it can be used for bank fraud:

- Fraudsters can tell that an infected PC is a business PC, not a home PC, so they'll often target it with more aggressive and sophisticated attacks.
- Fraudsters can watch keystroke logs to get a hold of passwords, etc. They may even intentionally lock out accounts to make the user re-enter passwords or security question answers.
- Using the passwords they've captured, fraudsters can log into web services like email and online banking to steal more information or initiate banking transactions.
- It's common for fraudsters to initiate large wire or ACH transfers to themselves if they gain access to online banking accounts. Many times, the transfers go to offshore accounts or bounce through a network of "mules" who quickly forward the funds out of reach, leaving the victim unable to recover them. In most cases, the funds are gone within the first day and before the fraud is discovered.

How To Prevent It

Sound scary? It is! And it's becoming more and more common. Preventing online bank fraud is shared responsibility – both you and your financial institutions should be taking steps to keep your information and your funds safe. Talk to your business partners to find out if they meet industry security standards including multi-level authentication. Johnson Bank clients can contact their Relationship Manager to learn more about our specific security features. Here are a few things your business can do to prevent malware from infecting your PCs:

- Keep antivirus and antispyware up-to-date.
- Apply all Microsoft security patches.
- Use good passwords (different passwords for different things) and protect passwords – ask all employees to do the same.
- Encourage employees not to use work computers for risky or non-work applications (no installing games or file sharing, limit web use to business sites, don't access personal email accounts).
- Take indicators and warnings seriously (PC antivirus alerts, locked password without reason, suspicious phone call digging for information, or just that "something wasn't quite right" feeling).
- Adopt stronger authentication, such as tokens or one time passwords. Note that Johnson Bank will begin offering security tokens in 2009.

