

Safer Banking Online

- 1) Use a dedicated system for financial transactions. If you're using a shared system that is not locked down, you might as well just cut the attacker a check. It would save time for everyone.
- 2) Use a dedicated firewall on the financial transaction system that is configured to only allow connections to your online banking IP and to necessary update sites.
- 3) Keep the workstation hardened and updated. Many attackers use Microsoft and Adobe vulnerabilities to get in. If you don't need Adobe, don't install it.
- 4) Take away admin rights. Use Windows 7 if you can. If you cannot, make sure that your users cannot install software.
- 5) Use a real antimalware program. Good business-level antimalware systems include Sophos (full control) and Kaspersky (antimalware only). Remember, whatever you pick, you get what you pay for. If you detect malware on your dedicated system, contact your bank immediately.
- 6) Set your account to use dual controls. If one person can set up transfers, but someone else has to approve them, the attacker's job becomes a whole lot more difficult.
- 7) Sign up for alerts so you are notified when transactions occur. If a transaction looks suspicious, notify your bank immediately.
- 8) If your bank supports PositivePay or Whitelisting, set it up. By approving specified recipients ahead of time, you reduce the ways in which attacks could steal your money.
- 9) If your bank allows you to do so, use transfer limits. By limiting the amount that an individual can transfer or that can get moved in a day/week/month, you reduce the amount of money that could be lost in a successful attack. Larger transfers can be approved manually.
- 10) If they are available from your bank, use tokens. You may need to request these from your bank and pay a small fee for each token. The protection that you gain is usually worth the cost.
- 11) Some banks have optional security software that will authenticate each transaction. Contact your bank to determine whether or not this is an option for you.

More information: <http://www.alliancetechnologies.net/blog/morej/protecting-yourself-malware>