Panda Security USA Study

THE EFFECT OF BANKING TROJANS ON SMALL AND MEDIUM-SIZED BUSINESSES IN THE UNITED STATES

By Sean-Paul Correll

Threat Researcher,
Panda Security

April 20, 2010

Executive Summary

The malware economy is flourishing and affecting both consumers and businesses of all sizes. The reality is that cybercrime is growing exponentially in frequency and sophistication. The following Panda Security study examines the prevalence and effects of cybercrime, specifically banker Trojans, on an increasingly targeted demographic: small and medium-sized businesses (SMBs). After a thorough survey of more than 300 high-level SMB executives across a wide range of industries, Panda Security found SMBs are lacking a solid level of awareness around the real risk that their businesses face, and more pressing, that they may not be as protected as needed to keep their assets and networks safe.

Panda Security found that while a majority of respondents are concerned about online banking fraud and identity theft in their organizations, they don't have a good understanding of how best to protect their businesses. In addition, they have a false sense of security in terms of their expectations around bank reimbursement in the unfortunate event they fall victim to fraud.

Overall, Panda Security's study revealed some compelling results:

- 66 percent of the 25 million malware samples collected by PandaLabs in 2009 were banker Trojans
- 52 percent of respondents had little or no familiarity with banking Trojans, despite the wave of increased attacks in 2009
- Small businesses continued to be a prime target for cybercriminals in 2009 as evidenced by the multiple attacks using banker Trojans such as URLZone
- 49 percent of survey respondents use online banking to make and receive payments online

- 11 percent of SMBs said they have or may have been affected by online fraud or identify theft, of which 86 percent were reported to authorities
- 15 percent either do not have updated security software on all systems where online transactions are conducted or are unsure of the status of their security software at their organizations

When looking at the evolving threat landscape, there are very few constants. Cybercriminals are continuously developing new exploit techniques, their methods for distributing malware are always evolving, and malware creation kits are becoming easier to use and more readily available. However, the one constant characteristic of the malware ecosystem is the cybercriminals' greed as they steal, harvest and sell financial information for their own financial gain. In 2009, PandaLabs detected a record number of new malware samples, highlighting the unrelenting cat and mouse game between the cybercriminals and those trying to fight them.

While the implications of cybercrime are very real for consumers, SMBs and large enterprises alike, Panda Security has seen a sharp rise in the volume and level of sophistication of targeted attacks against SMBs in particular.

SMBs are Sitting Ducks

According to PandaLabs' 2009 Annual Report, 66 percent of the 25 million samples Panda collected throughout the year were banking Trojans designed to steal financial and other personal information. This is a trend that Panda predicts will continue and has already seen evidence of the proliferation of banker Trojan samples in 2010. According to the Q1 2010 PandaLabs Report[1], Trojans accounted for 61 percent of all malware created during the three months of this year and continue to rank as the weapon of choice of cyber-criminals, through identify theft or stolen bank and credit card details. Once that information is stolen, it is resold on the black market to carry out various fraud schemes.[2] The Annual Report clearly demonstrates that users who are most vulnerable to banking Trojans are those who frequently conduct online banking, with small to medium-sized businesses being at particularly high risk. These organizations, ranging in size from one to 500 employees, are attractive targets because they are less aware of the myriad threats that exist and underprepared to protect themselves owing to more limited budgets and internal resources. Moreover, SMB accounts are particularly attractive to criminals because they have higher account balances than consumer accounts, yet lack the protections of larger enterprises.

There were several instances in 2009 that demonstrated just how vulnerable SMBs are. In September 2009, approximately $439,000 was stolen from German bank accounts with the aid of a sophisticated banking Trojan called URLZone.[3] The attackers stole banking credentials from the URLZone-infected systems, and then initiated money transfers through the victims' computer systems by using the stolen credentials. More recently, hackers were able to infiltrate and steal $150,000 from a small insurance company in Michigan.[4] Using the widely popular Zeus Crimeware Kit, attackers hacked into the controller's computer and initiated money transfers until the company's bank account was depleted. These are just two recent examples out of countless attacks that happen annually.

[1] http://www.pandasecurity.com/homeusers/security-info/tools/reports.htm

[2] http://www.pandasecurity.com/img/enc/Annual_Report_PandaLabs_2009.pdf

[3] http://www.scmagazineus.com/urlzone-touted-as-most-sophisticated-banking-trojan-yet/article/151096/

[4] http://www.krebsonsecurity.com/2010/02/hackers-steal-150000-from-mich-insurance-firm/#more-1087

Banking Trojans Defined

When referring to a banking Trojan, we define it as a piece of malware that targets money from an online banking account. Trojans can be downloaded onto PCs through various ways, such as malicious links on search engines, Facebook or Twitter, or through sophisticated phishing emails that trick recipients into clicking on the malicious links that download the Trojan onto the PC. An increasingly effective way for Trojans to be distributed is through botnets, such as the Mariposa botnet, a massive network of infected computers designed to steal sensitive information.[5] One of the most common infection methods for Trojans is a drive-by-download attack. The Trojan sites are typically coupled with exploits, such as the latest Internet Explorer zero-day vulnerability covered here: http://www.vimeo.com/10078939.

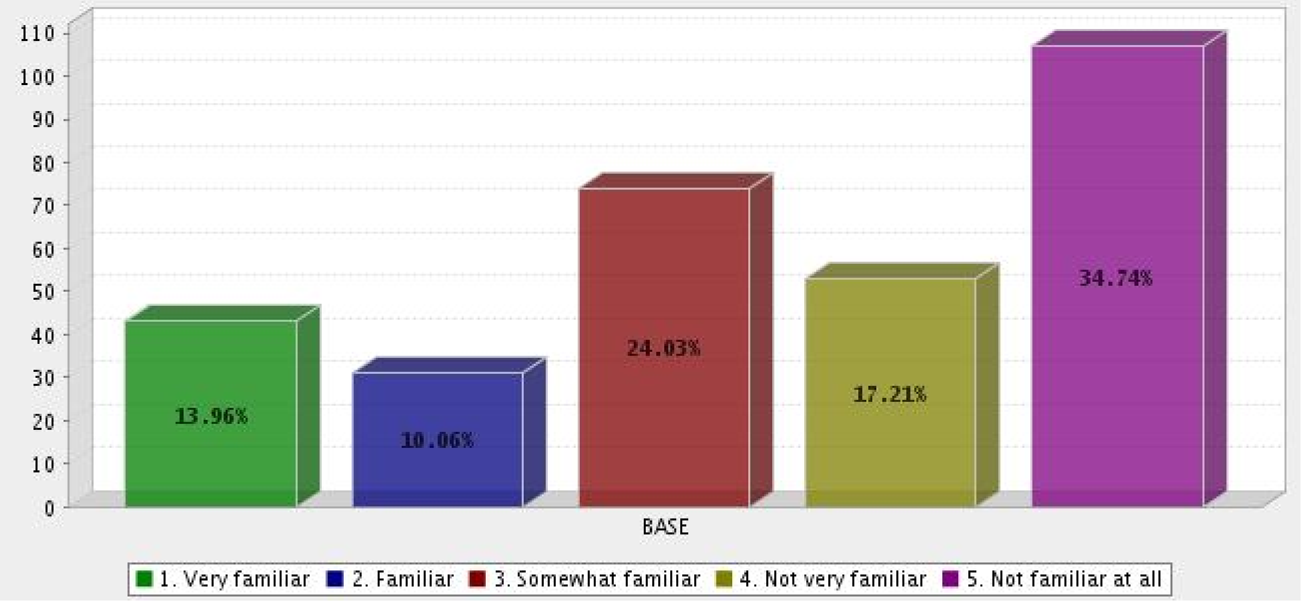
Once active on the machine, the banking Trojan waits until the user accesses an online banking site. After the Trojan has determined that the banking session has begun, it captures the user's credentials or the authenticated banking session. Trojans can take screenshots, capture videos, log keystrokes, or grab forms to capture information such as account numbers, signatures, check images and addresses. Some of the most famous banking Trojans in recent history are URLZone and Zeus.

The SMB Banking Trojans Survey: Purpose and Results

To understand in greater detail how vulnerable small businesses are to cybercrime, Panda Security conducted a comprehensive survey in January 2010. The purpose was to better understand the true effects of banking Trojans on SMBs, gauge awareness levels and bring attention to the growing impact of cybercriminal activity targeted at small businesses.

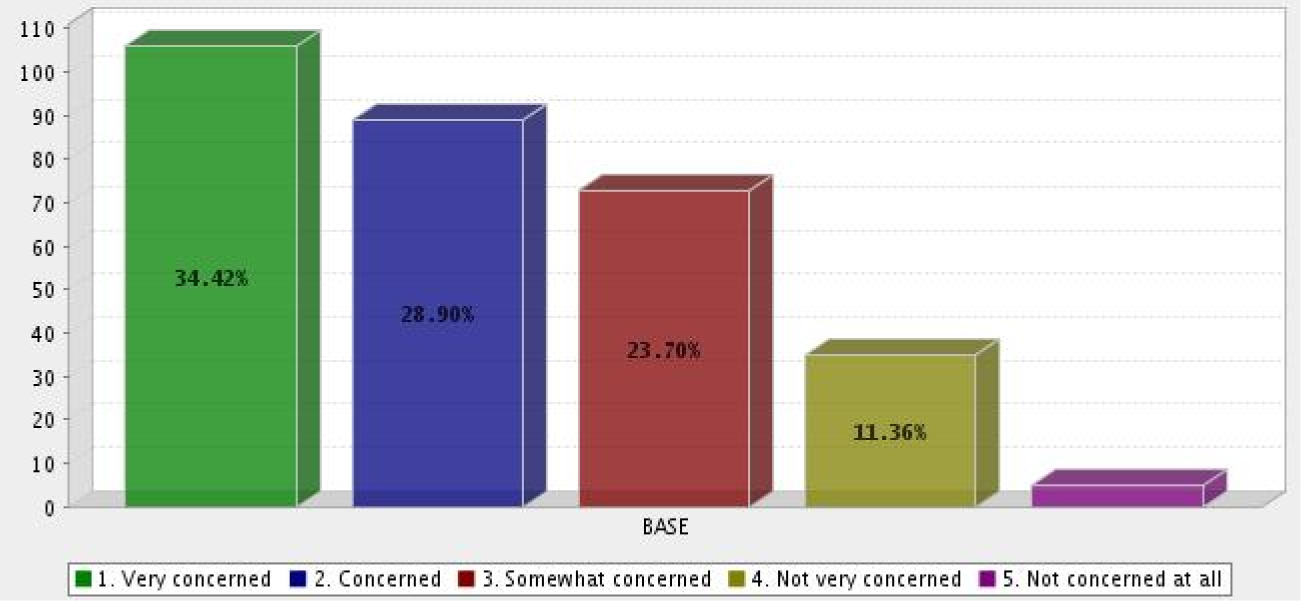
The survey consisted of 307 respondents from small to medium-sized businesses (2 to 250 seats) in the United States in executive and financial roles across 38 different industries, including finance, banking and retail. The survey was conducted online by Conduit Systems, LLC, and no Panda customers were involved. The error rate for a 307 sample size at a 95 percent confidence level is +/- 5.6. The results revealed that a majority of respondents (52 percent) had little or no familiarity with banking Trojans, despite the wave of increased attacks in 2009.

[5] http://www.pandasecurity.com/homeusers/media/press-releases/viewnews?noticia=10085



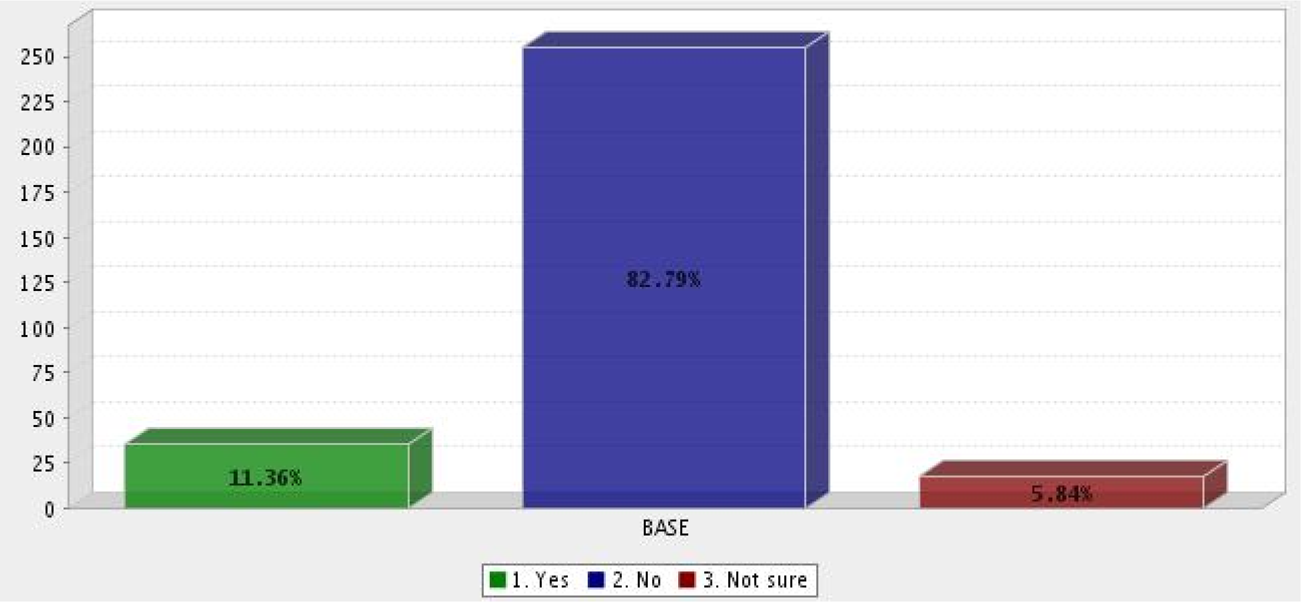
Survey Result -- How familiar are you with banking Trojans?

The lack of knowledge of financially motivated malware is alarming, especially considering that the majority of respondents (63 percent) said they are concerned about online banking fraud or identity theft in their organizations.



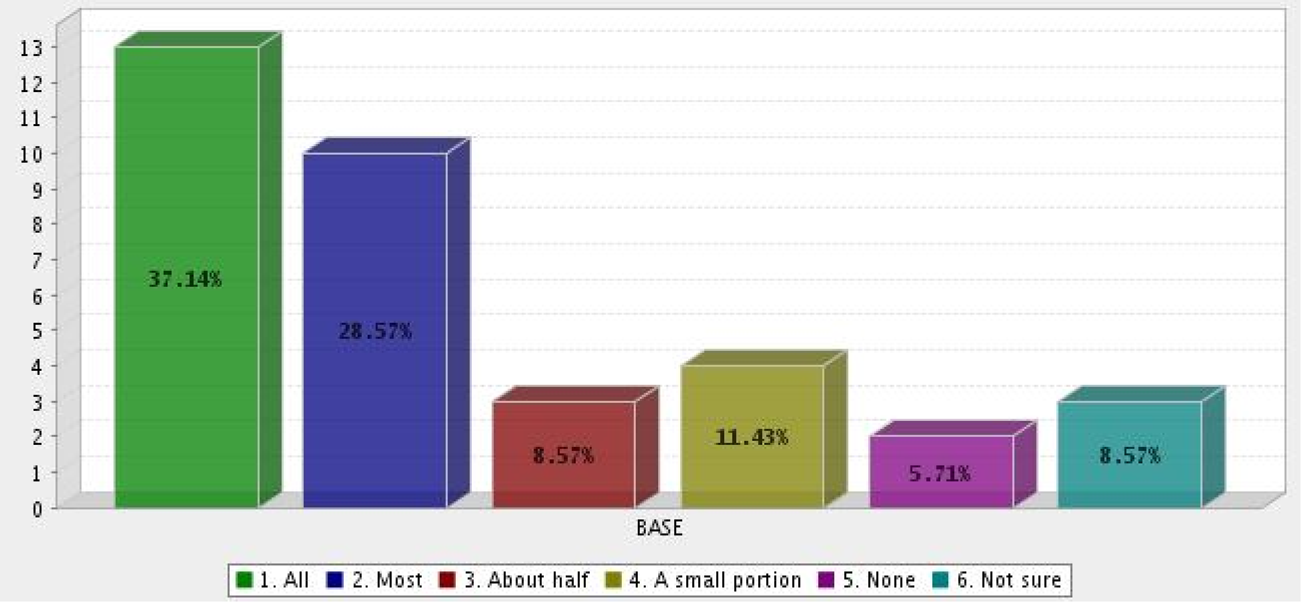
Survey result -- How concerned are you about online banking fraud and identity theft in your organization?

These results show that while organizations are concerned with online banking fraud and identity theft, they either don't have the resources dedicated towards properly addressing these threats, or are unsure of the best ways for protecting their systems. Small and medium-sized businesses have limited resources to dedicate to every aspect of running their companies successfully, and unfortunately, security can oftentimes assume a lower priority than it should. While Panda found in this study that 11 percent of SMBs said they have or may have been affected by online fraud or identify theft (of which 86 percent were reported to authorities), the company expects this number to rise as these businesses continue to be a prime target for attack.



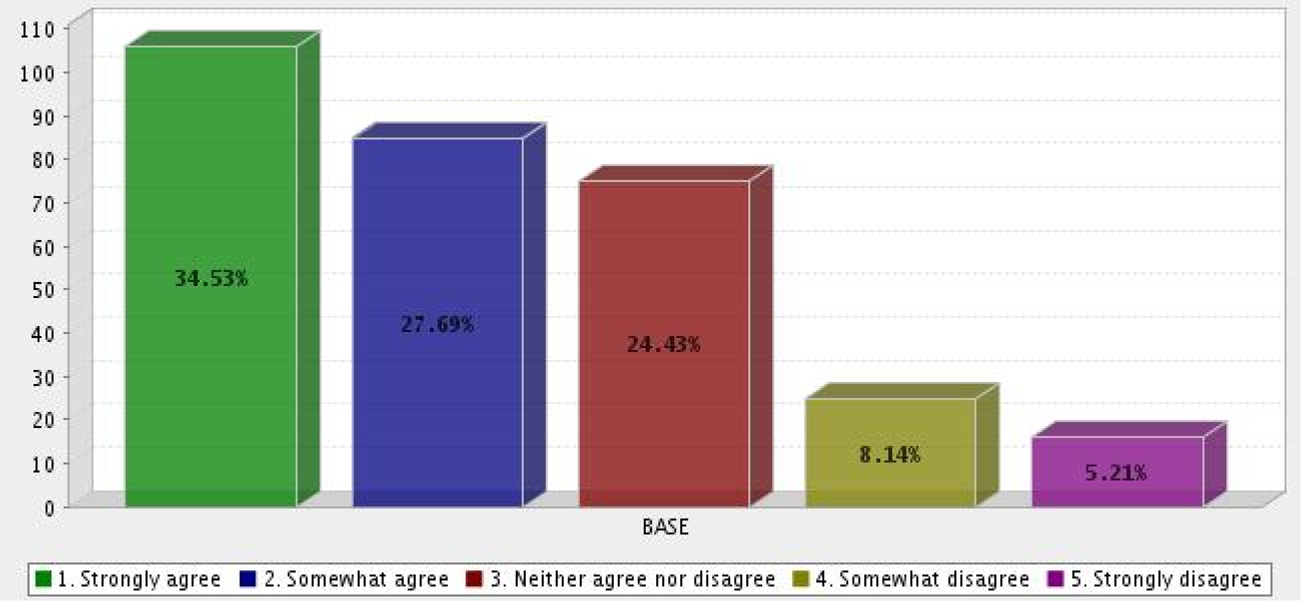
Survey result -- Has your business ever been the victim of any type of online fraud or identify theft?

Astonishingly, only 37 percent of the victims said all of the stolen funds were returned back, with 28 percent reporting that most of the stolen funds were reimbursed; 8 percent reporting half; 11 percent reporting a small portion; and 5 percent receiving none of the stolen funds. That means the vast majority of businesses affected by banking Trojans were not fully reimbursed by banks as they assumed they would be.



Survey result -- How much of the funds were returned back to the company?

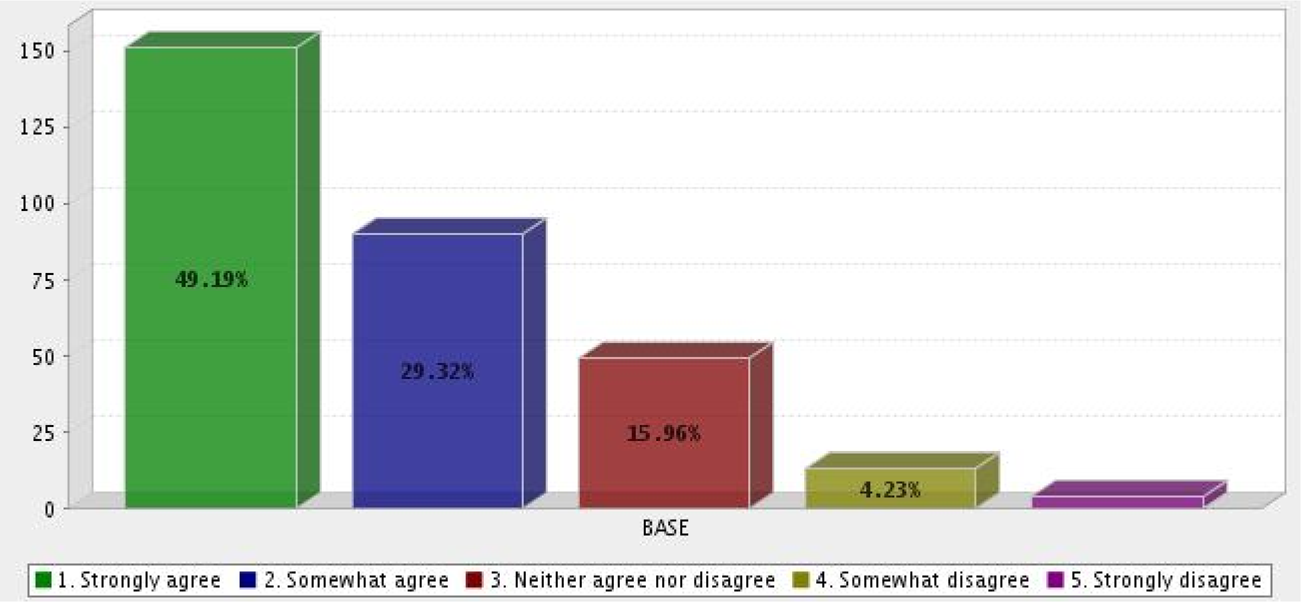
The report revealed a big gap between what cybercrime victims expect in the way of reimbursement from banks and the reality of what funds are actually returned. Sixty-three percent said they strongly or somewhat believe their bank would return all of the funds to their possession. This statistic is concerning because only 37 percent of the victims said all of the stolen funds were returned. While the majority of customers feel their banks should issue some sort of reimbursement for cybercrime, most (52 percent) also have little or no familiarity with the banking Trojans that are infecting their computers to begin with. It is apparent that businesses are generally not aware of the threats and believe that the bank will step in and save the day should they become victims.



Survey Result -- My bank would return all of my company's stolen funds back into my possession

Here are some additional highlights from the survey:

- 58 percent of respondents do not have insurance to protect their business from banking fraud and identity theft or are unsure if they do, while, 63 percent of the respondents still believe that stolen funds would be returned to their possession.
- 64 percent have protective and/or procedural methods in place at their organization to detect or prevent online banking fraud.
- 15 percent either do not have updated security software on all systems where online transactions are conducted or are unsure of the status of their security software at their organizations
- 49 percent use online banking to make and receive payments online.
- 78 percent strongly or somewhat agree that their bank would work with the authorities to pursue the perpetrators.



Survey Result -- My bank would work with authorities on my company's behalf to pursue the perpetrators

Conclusion and Next Steps

The primary conclusion from this study is that small and medium-sized businesses do not understand the risks well enough to protect themselves, and most have a false sense of security when it comes to expectations that financial institutions will reimburse them for stolen funds resulting from online fraud. As malware threats continue at a devastating pace, antivirus companies have to adapt and mature their malware collection, analyzing and classification systems to stay one step ahead.

In 2007, after observing the dramatic increase in malware threats, including banking Trojans, Panda developed and introduced Collective Intelligence technology[6], a proprietary technology that uses cloud computing to automatically analyze and classify thousands of new samples per day.

In 2009, Panda launched Panda Cloud Protection, a managed security solution for endpoints and e-mail aimed at the SMB market. Like all other Panda products, Panda Cloud Protection utilizes the Collective Intelligence technology to ensure customers are protected against the latest threats immediately. Unlike traditional security software, Panda Cloud Protection provides a fully hosted security service that can be managed by SMBs themselves, or their solution providers, removing the infrastructure costs typically associated with antivirus protection.

[6] http://www.pandasecurity.com/homeusers/solutions/collective-intelligence/

Staying Protected

Panda Security recommends the following protocol for all small and medium-sized businesses conducting financial transactions online:

1. Make sure your network is protected with up-to-date anti-malware software and set it to scan regularly.
2. If your security is managed by an outside IT service provider, inquire with them if the anti-malware protection is up-to-date.
3. Stay educated about the evolving tactics used by cybercriminals to steal from SMBs. Panda Security regularly publishes information about banking Trojans and other harmful malware in the PandaLabs blog: http://pandalabs.pandasecurity.com/.
4. Make yourself aware of the security and reimbursement policies put in place by your business' bank.
5. If possible, use a dedicated computer solely for making online banking transactions.

Small business owners who feel their systems have been compromised, or who would like to learn more about the SMB study, should visit: http://us.pandasecurity.com/criticalalert/ for additional support from a Panda Security professional.