



The Security Division of EMC

White paper

RSA 2010 Global Online Consumer Security Survey: United States Results



In the RSA 2010 Global Online Consumer Security Survey, we asked over 4,500 adults from 22 countries to share their opinions and attitudes on the online security risks they face, their level of awareness concerning the latest threats, and what online service providers should do to protect them.

Among those surveyed in the United States, the vast majority regularly visit and interact with online sites such as online banking, social networking and government and healthcare portals, with 97 percent conducting an online banking transaction and 93 percent making an online purchase in the last month.

This report will examine the results of the survey on a regional level, comparing the results of respondents from the United States to the overall global results. The report will summarize how aware consumers from these regions are to the online threats they face, analyze how consumer attitudes and awareness has transformed in light of changes in the way consumers use the Internet, and how the impact of strong authentication is directly correlated with consumer confidence and their willingness to conduct transactions and interact with online sites.

Consumers more aware of threats, but remain concerned

Consumers have expressed an increased awareness in many types of threats they face online each day. Banks and social networking sites, perhaps the two types of sites most targeted by online criminals, have been very proactive in providing ongoing user education. In addition, online fraud and cybercrime is of great interest to the media and has become a highly popular topic to report on in the news. The increase in consumer awareness can be attributed, at least partly, to the ongoing education offered by service providers and the media.

This is evident in the vast consumer awareness among many popular online threats. Among consumers in the United States, 82 percent indicated that they were aware of the threat of phishing and what it meant. Additionally, 89 percent stated that they were somewhat to very concerned with the threat of phishing, directly in line with the 89 percent that reported concern among global respondents.

Despite increased awareness, one in three consumers in the United States – or 31 percent – claimed they have been the victim of a phishing email attack. While consumer perception about being a phishing victim may vary – from whether they received a phishing email to whether they actually clicked on a link and provided personal information

to a phishing site – the percentage of American consumers that claimed to have been a victim of phishing is alarming nonetheless.

The large number of consumers in the United States that claim to have been a victim of phishing can likely be attributed to the more sophisticated and targeted attacks used by online criminals today. For example, many phishing emails today directly replicate the design of a legitimate communication from a bank, online retailer or other organization and lack the poor grammar that once made phishing attempts so obvious. Therefore, it is not a surprise that more consumers are falling victim to phishing scams.

In addition, the sheer volume of phishing attacks being launched today is also contributing to these trends. For example, based on the phishing statistics reported by the RSA Anti-Fraud Command Center, the United States and the UK were targeted by 80 to 90 percent of all phishing attacks in 2009. It can be concluded that for these reasons, we are not only witnessing increased concern among consumers, we have also seen an increase in effectiveness as demonstrated by the significant increase in the number of consumers that have admittedly fallen victim to a phishing scam.

An increase in consumer awareness is further evident from the number of respondents that expressed awareness of Trojans. In the United States, 73 percent of consumers stated that they were familiar with Trojans, only slightly lower than the global average of 81 percent.

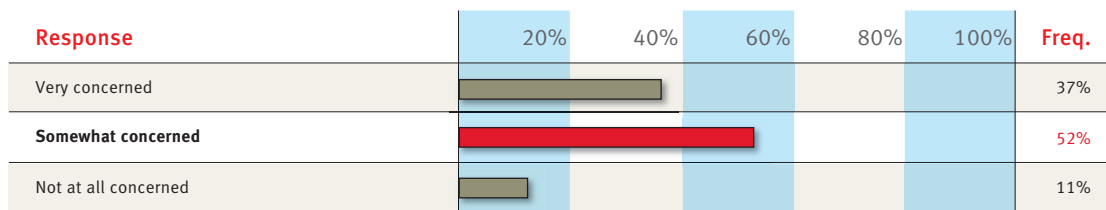


Table 1

How concerned are you about Phishing email attacks on your computer (by “Phishing” we mean emails that look like they are from a legitimate source, such as your bank, but are actually from a fraudster or cyber criminal trying to trick you into giving them your personal information)? (Respondents could only choose a **single** response.)

In addition, 95 percent of American consumers stated they were somewhat to very concerned with the threat of Trojans. This is not surprising as Trojans typically have a greater impact, are capable of collecting all types of information stored on an individual’s computer, and often go undetected by the consumer and even the anti-virus programs designed to stop them¹.

Consumers in the United States, while highly aware of phishing and Trojans, are not as savvy when it comes to newer threats such as vishing (voice phishing) and smishing (phishing via SMS or text messaging). Among those surveyed, only 28 percent were aware of vishing and 23 percent were aware of smishing. This is particularly concerning to RSA as we have witnessed the incidence of vishing and smishing rising rapidly. For example, the number of vishing attacks addressed by RSA increased fourfold in the last twelve months. This increase, coupled with a lack of awareness among consumers concerning these threats, makes it likely that these types of attacks will be a cause for concern in the United States over the next year.

Consumer concern is all over the Internet

Consumers have more threats to be concerned with, but have also brought more parts of their daily life to the Internet. Beyond online commerce and banking, there has been a dramatic increase in the way we communicate and network with others via social networking. Healthcare companies and local, state and federal government

agencies are also bringing the power and convenience of online services to the market.

To address the changes in online behavior that have occurred within the last two years, RSA surveyed consumers about their level of concern regarding their personal information being accessed or stolen at the various sites they visit and how their concerns impact their willingness to interact with those sites.

About four out of five consumers in the United States – or 79 percent – expressed that they were somewhat to very concerned with their personal information being accessed or stolen at their online banking site. This was slightly lower than the 86 percent of global respondents that stated they were somewhat to very concerned. However, consumers in the United States also expressed they were somewhat to very concerned with their personal information being accessed or stolen at other sites they visit such as healthcare portals (63 percent), government portals (65 percent), and social networking sites (62 percent).

This finding is interesting for a number of reasons. First, many financial institutions that offer online banking are diligent about online security for their customers and have already or started to implement some form of strong authentication to protect customer accounts from unauthorized access.

Second, it also indicates that consumers are most protective and place the most value in their financial information. However, they are likely unaware of what an online criminal can do with a full personal information profile and what the value is to them compared to a single bank account or credit card number. For example, the

¹ In September 2009, Trusteer reported that the Zeus Trojan, one of the most widely used pieces of malware targeting online users, was detected by anti-virus programs only 23 percent of the time.

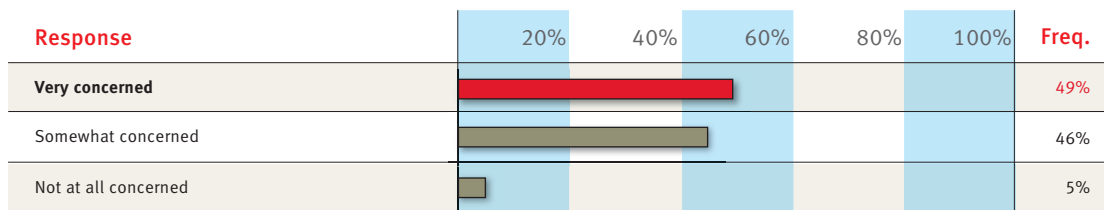


Table 2
 How concerned are you about Trojans and spyware being installed on your computer?
 (Respondents could only choose a **single** response.)

average selling price for a U.S. credit card in the fraud underground is \$1USD. But when that single card is sold with a full identity profile, which includes information such as the customer’s billing address, Social Security number, mother’s maiden name and date of birth, the price is inflated to \$20USD.

While consumers in the United States were concerned about their information being accessed or stolen at the various online sites they visit, they were not as hesitant to submit their personal information to those sites. For example, while 79 percent expressed they were concerned about their personal information being accessed or stolen at their online banking site, only 51 percent said those concerns might impact their willingness to submit personal information or interact with the site.

The impact on consumer willingness to submit personal information or interact with other types of sites was similar for government (49 percent) and healthcare (54 percent) portals, but higher for social networking sites (64 percent).

Consumers most concerned about online and mobile banking

Financial institutions interact with their customers across multiple touch points – online, over the telephone, on mobile devices, and at ATMs and branches. Not surprisingly, online banking still garners the most concern among consumers. As demonstrated in the previous section, 79 percent of respondents in the United States

stated they were somewhat to very concerned with their personal information being accessed or stolen at their online banking site. As a result, 66 percent of those same respondents also stated that banks should implement a stronger form of security to identify users when they log into online banking. This was lower than the 80 percent of consumers globally that called for stronger security for online banking.

Consumers also responded that they expected their banks to conduct some level of transaction monitoring on their online banking accounts to detect unusual activity. Among those surveyed in the United States, 92 percent stated they expect their banks to monitor their online banking transactions. Overall, the expectation of consumers to have their online banking transactions monitored did not differ significantly on a global basis, despite the different perceptions of privacy and security among the various regions we surveyed.

Mobile banking presents concerns for consumers as well. Among those surveyed that use mobile banking, 47 percent indicated they felt secure when using it, with only 14 percent responding “very” secure. While just under half of American consumers reported they felt secure using mobile banking, concern is likely to grow in the coming year as criminals develop ways to launch attacks against this new and growing population.

Among mobile users in the United States, 80 percent stated that banks should implement a stronger form of security for mobile banking. The desire for strong authentication for mobile banking did not vary much by region.

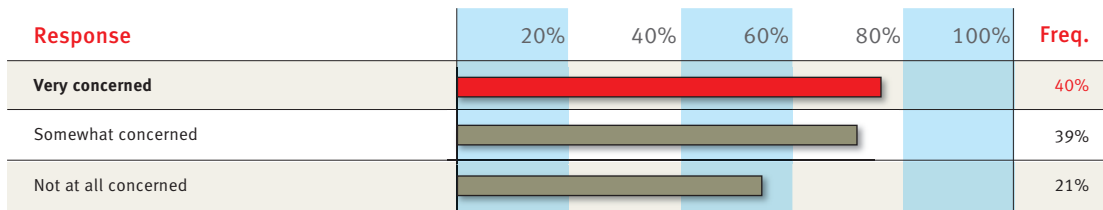


Table 3

Question: What is your level of concern with your personal information being accessed or stolen at an online banking site?

Consumers in the United States showed the greatest concern over the security of mobile and online banking compared to more traditional methods of interaction such as using telephone banking. Among those surveyed, 75 percent of respondents felt somewhat to very secure using the telephone banking system offered by their bank.

While the sense of security when using telephone banking was higher than online or mobile banking, consumers in the United States still felt that banks should use stronger security within this channel; 71 percent stated stronger security should be used to identify customers using the telephone banking system.

Consumers want security over convenience

One of the barriers organizations face in implementing strong authentication is the impact it will have on customer usability. The purpose of migrating services to the online channel is to reduce costs and provide added convenience for customers. However, the question still exists: Will

adding strong authentication compromise usability and have an impact on customer adoption? Organizations are always walking a fine line in an attempt to balance security, convenience and usability.

Consumers have become accustomed to stronger authentication from conducting banking transactions and making purchases online. Many financial institutions and merchants have already implemented or are starting to implement some form of strong authentication on their websites in an attempt to protect consumer identities and the activities they perform.

When asked how willing they would be to use a new security method if it was offered by their bank, 97 percent of consumers stated they would be somewhat or very willing to use it.

The same concepts that apply to online banking also apply to other websites that consumers are starting to use more and more – from online healthcare and government portals to social networking sites.

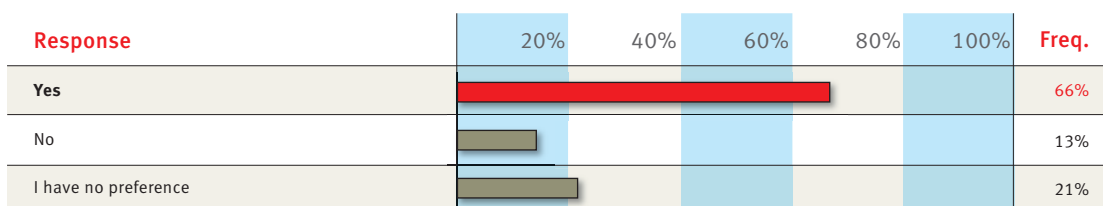


Table 4

Do you think that banks should implement a stronger form of security to identify users (other than a username and password) when they log into online banking?

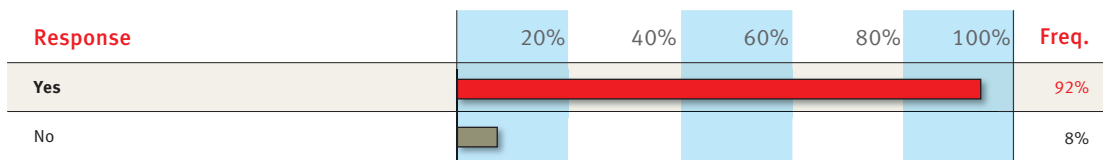


Table 5

Do you expect your bank to monitor your Internet banking activities and detect and confirm suspicious activity (e.g. an unusual money transfer)?

Healthcare portals

Healthcare providers are increasingly offering their patients new services through the use of online portals. From these portals, patients can access their personal medical history and information, review results from recent tests, schedule appointments and perform other activities that generally require a phone call or visit to the doctor’s office.

Consumers were asked if online healthcare sites should use a stronger form of security to identify users, beyond a username and password, when users are logging in to their portal. Among respondents in the United States that access a healthcare portal regularly, 54 percent stated that healthcare portals should use a stronger form of security to identify users. However, among those same respondents, 94 percent stated they would be willing to use a stronger form of security if it was offered.

Government portals

Federal and local governments are also increasingly offering new services online to citizens. From registering their vehicles and renewing a driver’s license to applying for certain benefits, government portals have started to migrate services to the Internet in an attempt to reduce costs and serve citizens more effectively.

Consumers were asked if online government sites should use a stronger form of security to identify users, beyond a username and password, when users are logging in to their portal. Among respondents in the United States that access a government portal regularly, 67 percent stated that government portals should use a stronger form of security to identify users. And as with healthcare portals, a vast majority – or 97 percent of consumers – responded they would be willing to use a stronger form of security if it was offered.

Social networking sites

Social networking sites have become a hotbed for online criminals because the number of users that engage in social networking activities continues to grow at unprecedented rates. The heavy traffic and global reach of these sites have made them a prime target for exploitation by criminals who seek to spread malware, launch phishing attacks and hijack accounts to spam other users. It is estimated that nearly 20 percent of online attacks are targeted at social networking sites².

Nearly five out of ten consumers in the United States – or 48 percent – felt that social networking sites should offer a stronger form of security to identify users although 94 percent would be willing to use it if it was offered.

The number of consumers that felt online banking sites should offer a stronger form of security to identify their users was higher compared to those that felt healthcare and government portals and social networking sites should offer a stronger form of security to identify their users. Once again, this demonstrates the value that consumers place in their financial information over other personal information and perhaps a lack of awareness about the types of fraudulent activities that criminals can perform by just having access to general personal information. In addition, these figures may indicate that consumers are not aware that the numbers of attacks against these other types of sites are increasing rapidly.

While the number of American consumers that felt other sites should offer stronger security were lower compared to online banking, the majority still felt that stronger security should be offered. Equally as important, consumers overwhelmingly expressed a willingness to use it if it was offered. As online users start to perform more activities that involve the use of their personal information on the Internet, we expect the number of consumers that want stronger security at these sites to grow.

² Breach Security Labs, Web hacking Incidents Database 2009 Bi-Annual Report

Online security inspires confidence

Online commerce is perhaps the oldest form of online “service.” Yet, retailers still face the same barriers in trying to convert traditional brick-and-mortar shoppers to make purchases online. In one survey after another regarding the topic, security is most often cited as the primary reason some consumers are hesitant to shop online; they are afraid of submitting personal and financial information over the Internet.

Consumer confidence can be directly attributed to increased transactions. In order to gain that confidence, providers of an online website and portal – whether offered through a retailer, bank, or healthcare organization – must consider security a key driver to adoption. To demonstrate, one major U.K. bank that deployed strong authentication to their online users reported a 20 percent increase in the number of transactions performed online only one month after the system was launched³.

RSA found that consumer confidence and the willingness to transact online was clearly correlated. In the United States, when consumers were asked, in general, how stronger security would impact their confidence in transacting online, 83 percent stated they would be more confident, with 42 percent stating they would be significantly more confident and 41 percent somewhat more confident.

How is stolen personal information being used to commit fraud?

The Travelers Companies, a major provider of insurance products and services in the U.S. and other international markets, analyzed data on the identity theft claims they addressed from 2008. Of all the cases they examined, they found that stolen personal information was used more than 75 percent of the time to open a new credit card account or make charges with cards on existing accounts.

When asked how stronger security features would impact their willingness to interact, purchase items, and submit personal information to the sites they regularly visit, 59 percent said they would be more likely to interact and submit personal information online.

Conclusion

The types of threats targeting online users continue to evolve everyday. As quickly as consumers become familiar with the threats they face and change their online behavior,

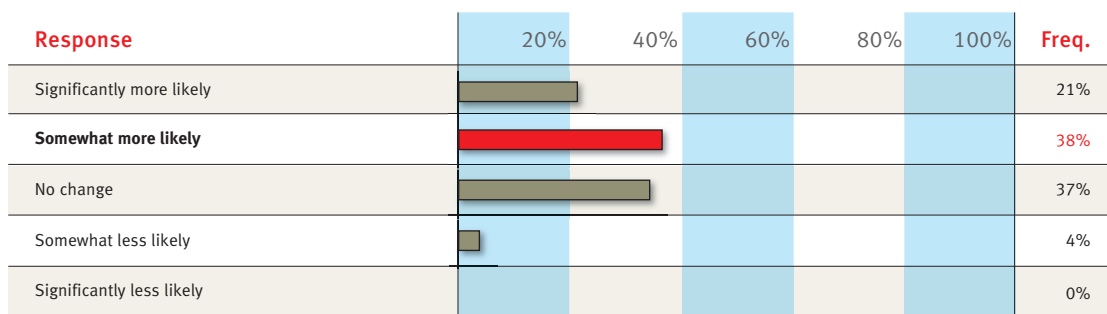


Table 6

How would any new security features, offered in addition to a username and password, impact your willingness to interact, purchase items, or submit personal information to the sites you regularly visit? (Respondents could only choose a **single** response.)

³ See RSA Case Study, “Alliance and Leicester: Accelerating Online Banking with Increased Security”

the criminals that seek to steal their personal and financial information also change their tactics. Consumer education and awareness is one of the first lines of defense in the ongoing battle against online crime.

Organizations will continue to take advantage of the many benefits offered by the Internet and consumers will continue to seek the convenience offered through the online channel – all despite the inherent risks. However, in order to maximize the full value of what the online channel can offer, organizations need to understand what it takes to launch a successful online portal that consumers will be willing to visit and use.

The online channel is a two-way street. Just because an organization offers its customers the convenience of online services, it does not mean they are going to use it. They

need to feel secure when they log in and submit personal and financial information. In our global survey of 4,500 consumers, including over 200 respondents from the United States, we found that a vast majority of consumers are concerned about the security of the websites they visit and about their information being accessed or stolen on those sites. We also found that most consumers feel some form of stronger security, beyond a simple username and password, should be implemented at the websites they interact with on a regular basis. This was true not only for online banking sites, but also for healthcare, government and social networking sites.

Finally, we found that offering stronger security at online sites inspires confidence and increases the likelihood that consumers will be willing to interact with and submit personal information to those sites.

About RSA

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.



The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

RSA and RSA Security are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products or services mentioned are trademarks of their respective owners. ©2009 RSA Security Inc. All rights reserved.

CSV WP 0110 US