



The Security Division of EMC

White paper

# RSA 2010 Global Online Consumer Security Survey: European 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.

Within Europe, over 1,800 respondents participated and were represented from the following countries: France, Germany, Italy, Poland, Spain, Sweden, Switzerland, the Netherlands, and the UK. Among those surveyed, the vast majority regularly visit and interact with online sites such as online banking, social networking and government and healthcare portals, with 92 percent

conducting an online banking transaction and 80 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 European countries to the overall global results. The report will summarize how aware European consumers 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 Europe, 81 percent indicated that they were aware of the threat of phishing and what it meant. This figure is slightly higher than the 76 percent of global respondents that expressed they were familiar with phishing.

Just as awareness of phishing in Europe is high, consumers also expressed concern over the threat. Among respondents from Europe, 83 percent stated they were somewhat to very concerned with the threat of phishing, only slightly lower than the 89 percent of global respondents that expressed concern.

Some countries, however, demonstrated a higher level of concern for phishing than others. For example, 90 percent of respondents from the UK and 85 percent of respondents from Italy stated they were concerned about the threat of phishing as compared to only 62 percent of respondents in Sweden and 78 percent in the Netherlands. This might be attributed to the number of attacks targeted at consumers in the UK and Italy compared to other European countries. For example, based on the monthly phishing statistics reported by the RSA Anti-Fraud Command Center, in 2009, the UK and Italy have consistently been among the top five countries experiencing the most volume of phishing attacks.

Despite increased awareness, consumers in Europe continue to be targeted, with 27 percent claiming they had 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 consumers that claimed to have been targeted is alarming nonetheless.

Most interesting was the number of consumers claiming to have been the victim of a phishing attack within various countries. In Italy, an astonishing 59 percent of respondents claimed to have been a victim of a phishing attack. This number seems to correlate directly with what RSA has reported over the past year in terms of Italy being one of the countries that we consistently witness suffering from the highest volume of phishing attacks. Among other European countries surveyed, Spain came in second with 45 percent of consumers stating they have been a victim of a phishing attack, followed by France (32 percent) and the UK (26 percent).

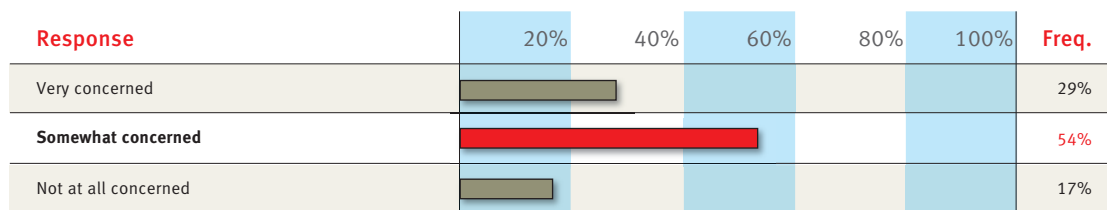
The large number of consumers in Europe that claim to have been a victim of phishing can likely be attributed to the more sophisticated and targeted attacks used by online criminals. For example, many phishing emails today directly replicate the design of a legitimate communication from a bank, online 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. The RSA Anti-Fraud Command Center recently reported record-breaking figures for three months in a row in terms of the number of phishing attacks they had identified in a single month<sup>1</sup>. 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 online users 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 Europe, 84 percent of respondents stated that they were familiar with Trojans, only slightly higher than the global average of 81 percent. However, among all the countries that responded, consumers in Germany (98 percent) and Poland (97 percent) expressed the greatest awareness.

Just as awareness of Trojans in Europe is high, concern over the threat is even higher as 88 percent of consumers expressed they were somewhat to very concerned with a Trojan being installed on their computer, with 38 percent expressing they were “very” concerned.



**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.)

<sup>1</sup> Between August and October 2009, the RSA Anti-Fraud Command Center reported record-breaking figures for the number of phishing attacks they identified in a single month. For more information, please refer to RSA’s monthly online fraud report.

Many financial institutions in Europe have been offering strong authentication to the consumer market for many years. However, online criminals have attempted to work around the security measures implemented at most online banking sites through the use of man-in-the-middle and man-in-the-browser Trojans which are designed to capture login credentials in real-time. The numbers of these attacks have been on the rise over the last two years, especially in Europe where two-factor authentication is widely deployed.

Consumers in Europe, 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 27 percent were aware of vishing and 33 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 types of threats, makes it likely that these types of attacks will be a cause for concern in Europe over the next year.

### Consumer concern is all over the Internet

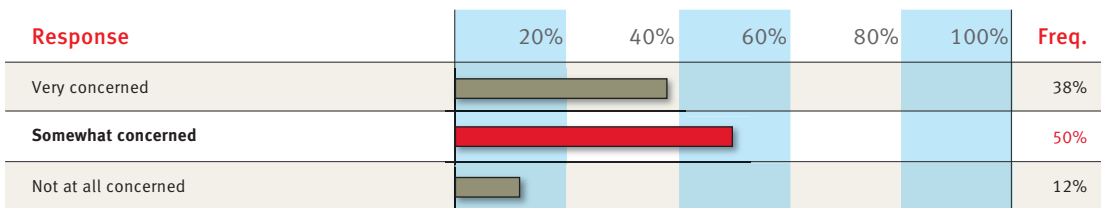
Consumers have more threats to be concerned with, but have also brought more parts of their daily life to the Internet. Beyond online commerce and banking, there has been a dramatic increase in the way we communicate and network with others via social networking. Healthcare companies and local, state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

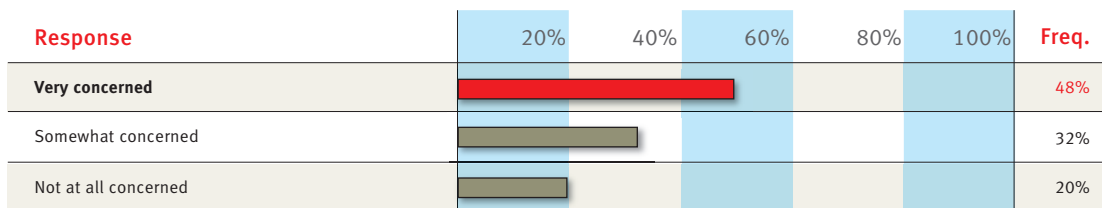
Overwhelmingly, consumers in Europe expressed they were somewhat to very concerned with their personal information being accessed or stolen at their online banking site (80 percent). This was only slightly lower than the 86 percent of global respondents that stated they were somewhat to very concerned. However, consumers in Europe 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 (57 percent), government portals (75 percent), and social networking sites (74 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 implemented some form of strong two-factor 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 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



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



**Table 3**  
 What is your level of concern with your personal information being accessed or stolen at an online banking site?

as the customer’s billing address, Social Security number, mother’s maiden name and date of birth, the price is inflated to \$20USD<sup>2</sup>.

While consumers in Europe were concerned about their information being accessed or stolen, they were not as hesitant to submit their personal information to those sites. For example, while 80 percent of users expressed they were concerned about their personal information being accessed or stolen at their online banking site, only 60 percent said those concerns might impact their willingness to submit personal information or interact with those sites. Surprisingly, consumers in France expressed the most trepidation with 87 percent of respondents stating their concerns over their information being accessed or stolen directly impacts their willingness to interact with their online banking site.

The impact on their willingness to interact with other sites was only slightly lower at social networking sites (56 percent) followed by healthcare and government portals at 53 percent each respectively.

One interesting observation can be drawn from analyzing the results from Sweden. The results of the survey at both the global and European levels showed consumers were most concerned with their information being stolen or accessed by an unauthorized person at an online banking site. They also conveyed those concerns impacted their willingness to interact with an online banking site. However, consumers in Sweden were unusual in that they were most concerned with their information being accessed or stolen at a social networking site and those concerns were much more likely to impact their willingness to interact with a social networking site (50 percent) versus an online banking site (30 percent).

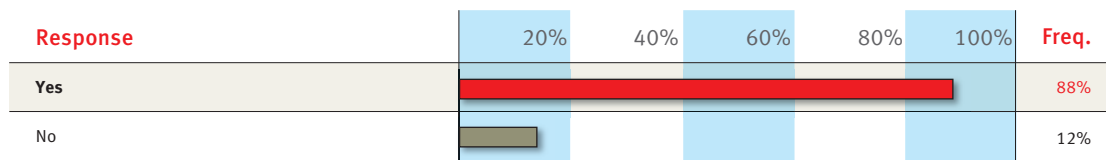
### Banking customers most concerned about online and mobile threats

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, 80 percent of respondents in Europe stated they were somewhat to very concerned with their personal information being accessed or stolen at their online banking site. As a result, 75 percent of those same respondents also stated that banks should implement a stronger form of security beyond a username and password when they log into 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 European consumers, 88 percent stated they expect their banks to monitor their online banking transactions.

This figure is important, especially in Europe where two-factor authentication such as one-time password tokens, EMV-CAP, iTan and mTan are widely used in the consumer market. Concerns over privacy are an ongoing issue in Europe, but when it comes to security, consumers are very willing to accept ongoing monitoring of the transactions they perform to ensure the protection of their financial accounts. 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.

<sup>2</sup> Source: RSA Anti-Fraud Command Center



**Table 4**  
Do you expect your bank to monitor your Internet banking activities and detect and confirm suspicious activity (e.g. an unusual money transfer)?

Mobile banking presents its own set of concerns for consumers as well. Among those surveyed that use mobile banking, only 46 percent indicated they felt secure when using it, with only 12 percent responding very secure. While nearly half of respondents in Europe reported they felt secure using mobile banking, consumer concern is likely to grow in the coming year as fraudsters develop ways to launch attacks against this new and growing population.

Among mobile users in Europe, 88 percent stated that banks should implement a stronger form of security for mobile banking. The desire for stronger authentication for mobile banking did not vary much by region.

Consumers in Europe showed the greatest concern over the security of online and mobile banking compared to more traditional methods of interaction such as using telephone banking. Among those surveyed, 67 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 still felt that banks should use stronger security within this channel. In Europe, 75 percent of consumers felt 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 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, 98 percent of consumers stated they would be somewhat or very willing to use it. And among consumers in each specific country, at least 90 percent of those who responded displayed a willingness to adopt stronger security for online banking. One hundred percent of consumers in Italy, Spain, Switzerland and the UK stated they would be willing to use stronger security if it was offered by their bank.

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.

### 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 from Europe that access a healthcare portal regularly, 58 percent stated that healthcare portals should use a stronger form of security to identify users. However, among those same respondents, 93 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 that access a government portal regularly, 62 percent stated that government portals should use a stronger form of security to identify users. And as with healthcare portals, a vast majority – or 94 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 sites<sup>3</sup>.

Despite this, only 48 percent of consumers felt that social networking sites should offer a stronger form of security to identify users although 87 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 (75 percent) was much higher compared to those that felt healthcare (58 percent) and government (62 percent) portals and social networking sites (48 percent) 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.

### 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.

While the number of consumers surveyed in Europe 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 more consumers start to perform activities that involve the use of their personal information at other online sites (beyond online banking and ecommerce transactions), we expect the number of consumers that want stronger security at these sites to grow.

### 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 launched<sup>4</sup>.

<sup>3</sup> Breach Security Labs, Web hacking Incidents Database 2009 Bi-Annual Report

<sup>4</sup> See RSA Case Study, "Alliance and Leicester: Accelerating Online Banking with Increased Security"

RSA found that consumer confidence and the willingness to transact online was clearly correlated. In Europe, when consumers were asked, in general, how stronger security would impact their confidence in transacting online, 88 percent stated they would be more confident, with 48 percent stating they would be significantly more confident and 40 percent somewhat more confident.

When asked how stronger security features, offered in addition to a username and password, would impact their willingness to interact, purchase items, and submit personal information to the sites they regularly visit, 66 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, 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 survey among more than 1,800 consumers within Europe, we found that a vast majority 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 logging in with just a 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 consumer confidence and increases the likelihood that they 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](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).



The Security Division of EMC

RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://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 1209 EUROPE