

Spaniards trust Internet banking

INTECO releases the results of the “Study on Online Fraud”, which analyses the monthly evolution of this phenomenon in the last three years.

- **The used methodology combines quantitative techniques based on the perception of Internet users (32,484 surveys distributed into eight data captures from 2007 to 2009) and real objective incidence measurements based on the 128,325 remote security analyses carried out monthly in home computers by the Information Security Observatory over this time period.**
- **The diagnosis is completed and enriched by information coming from the INTECO-CERT Online Fraud Repository, which gathers technical data from the incidents the INTECO-CERT itself and the Internet User Security Office detect.**
- **The area of Reactive Services and Operations of the INTECO-CERT detected 1,846 cases of phishing in 2008 and 1,959 in the first three quarters of 2009. Likewise, it identified 2,191 fraudulent URLs in 2008 and 1,810 in 2009 (until September).**

The level of trust in the Internet to carry out financial transactions is high: approximately 6 out of 10 users show great or enough confidence in using online banking.

Phishing in figures

The area of Reactive Services and Operations of the INTECO-CERT detected 1,848 cases of phishing in 2008 and 1,959 in the first three quarters of 2009. Likewise, it identified 2,191 fraudulent URLs in 2008 and 1,810 in 2009 (until September). The data analysed in 2009 suggest a trend of stability as compared to 2008.

At the national level, only 0.04% of the 1,082,757 .es domains existing in 2008 were linked to online fraud attempts. This trend has showed a positive evolution, since the percentage of fraudulent URLs of the 1,207,832 .es domains existing in 2009 has not exceeded 0.025%.

The number of fraudulent websites hosted on Spanish servers is equally low: 134 in 2008 (6.1% of the total) and 178 between January and September 2009 (9.8% of the total). Cybercriminals generally use external servers, which they compromise by exploiting vulnerabilities in some of their software products. The reduction in the number of fraudulent URLs hosted in Spain must be achieved through improving the procedures of monitoring and updating the systems and applications supported by the services.

Incidence of online fraud among Spanish users

The electronic mail is positioned as the most used channel for fraud attempts, whereas SMSs and direct calls have lower incidence. The most usual fraud methods are the linking to fraudulent websites, the offer of products and services that have not been contracted, fake job offers and requests for passwords via email.

In the 3rd quarter of 2009, most of the fraudulent communications (44.4%) received by the users came from a supposed bank. Behind this type of fraud, we can find those related to fake lottery and gambling websites (33,7%), online shopping websites (29,3%), telecom operators (21,8%), social networks (20,7%) and online auction websites (16,5%).

In the 3rd quarter of 2009, barely 3.8% of Spanish Internet users state to have suffered financial damage as a result of online fraud events. Nevertheless, most of the economic losses caused by fraud are of a small amount: 44.4% of the cases are classified as micro-frauds not exceeding €110.

Connection between fraud and e-Trust

Online fraud has two direct consequences for users: firstly, the tangible financial loss when the cybercriminal achieves his/her purpose; secondly, the user's possible loss of confidence after being victim of a fraud event. This latter effect, perhaps less mentioned than the former, is by no means trivial and influences the development and consolidation of the Information Society

The level of trust in the Internet to carry out financial transactions is high: approximately 6 out of 10 users show great or enough confidence in using online banking.

In spite of this substantial level of trust in the Internet as a channel to carry out economic transactions, citizens are still showing greater confidence in using this service in person. However, there is an upward trend: the percentage of citizens showing great or enough confidence in operations involving payments and economic transactions through the Internet is increasing quarter after quarter.

The fact of having being subject of a fraud attempt (not completed) does not affect the user's online shopping and banking habits significantly: 83.3% of the users do not change their online shopping habits and, 90.3%, their online banking habits, after having experienced a fraud attempt.

Abandonment rates are certainly small (around 4%), even among citizens who have suffered economic losses, which, apparently, is a sign that both services, especially the banking, have become highly indispensable for their users. This indicator must be taken into account, since it represents a highly reliable sign of the level of e-Trust of citizens.

About the National Institute of Communication Technologies (INTECO)

The National Institute of Communication Technologies, PLC (INTECO) is a state-owned organization attached to the Ministry of Industry, Tourism and Trade (MITYC) through the State Secretariat for Telecommunications and for the Information Society (SETSI)

INTECO's mission is to bring value and innovation to citizens, companies, public administrations and to the IT sector through the development of projects that contribute to strengthening trust in the Information Society services in Spain, whilst also promoting a line of international participation. Consequently, INTECO develops actions according to its strategic lines: Security, Accessibility and ICT Quality.

The Institute houses the Internet User Security Office, the Security Incident Response Centre, the Information Security Observatory, the SME Security Demonstration Centre, the Reference Centre for Web Standards and Accessibility and the National Laboratory of Software Quality, among others.

More information: <http://www.inteco.es>

About the Information Security Observatory

The Information Security Observatory is part of INTECO's strategic line of action regarding security and e-Trust.

The Observatory emerged with the purpose of describing thoroughly and systematically the level of security and trust in the Information Society, building specialized knowledge in the field, as well as preparing recommendations and proposals which define valid trends for future decision-making processes on the part of the industry and public authorities. Therefore, it is in the service of citizens, companies and Spanish public administrations to describe, analyse, advise and disseminate the culture of information security and e-Trust.

More information: <http://observatorio.inteco.es>

About the INTECO-CERT: Security Incident Response Center

The Security Incident Response Centre (INTECO-CERT) was established as a result of the *Plan Avanza* initiatives, with the aim of meeting the need of providing support in computer and information security issues both to citizens and to the Spanish industrial tissue.

Included in the area of Programmes of INTECO, it provides public services of prevention, information, awareness-raising, advice and support in issues regarding IT security to Spanish citizens and companies.

The Online Fraud Repository is part of the INTECO-CERT platform for managing the fight against online fraud. This platform enables the handling of online fraud incidents reported to the INTECO-CERT and to the Internet User Security Office, gathering related technical information which can be consulted later in the electronic fraud repository.

The INTECO-CERT Online Fraud Repository compiles structured information of all types of fraud from the detected cases and incidents, detailing the technical information of the electronic resources and services used and/or affected.

More information: <http://cert.inteco.es> and <http://www.osi.es>