How to shop safely online

December | 10

enisa
European Network and Information Security Agency

About ENISA

ENISA is an agency of the European Union, established to contribute to a high level of network and information security within the EU by:

- Giving expert advice on network and information security to national authorities and EU institutions
- Acting as a forum for sharing best practices
- Facilitating contacts between EU institutions, national authorities and businesses

Together with EU institutions and national authorities, ENISA seeks to develop a culture of security for information networks across the EU. This report and other ENISA reports can be found on ENISA's website (http://enisa.europa.eu).

Acknowledgements

Several parties supported and contributed directly or indirectly to this work in a number of ways. ENISA wishes to acknowledge the efforts of the members of the AR Community and their organisations, Brian Honan of BH Consulting, Daniel Blander of Palsit, Matthew Pemble of Idrach Ltd., Mathieu Gorge of Vigitrust Ltd., Nicola Fabiano of Studio Legale Fabiano, Fabio Guasconi of Mediaservice.net, Victoria Henry and Rebecca Landsdell from VeriSign Authentication (Symantec), Hans Pongratz of Munich's Technical University (TUM), Joao Moita, Isabelle Rodrigues of Anacom, Paul Pelsmaeker of Helder Resultaat, , Jorge Chinea López of INTECO and Javier Morant of CSIRT-Valencia (CSIRT-CV), who provided valuable inputs, material and prompt support for the compilation of the paper.

Finally, we would also like to acknowledge and to thank Paulo Coelho of KPMG, Jorge Pinto of Banco Credibom SA, and Georgios Raikos, who contributed to this document with informal reviews, valuable insights, observations and suggestions. The content would be incomplete and incorrect without their help.

Contact details

Katerina Christaki, Digital Communications Officer (katerina.christaki@enisa.europa.eu),

ENISA spokesperson: Ulf Bergstrom (ulf.bergstrom@enisa.europa.eu).

Table of Contents

Executive summary

The increasing availability of high speed networks, access to computers, a more technology aware consumer and ever improving online shopping environments has led to a continuous rise in the use of the Internet by consumers and retailers to buy and sell products and services online.

The online marketplace offers many advantages over the traditional physical, or "bricks-and-mortar", shopping environments. For the consumer, it provides the ability to shop at any time, from any place that has an Internet connection, such as their home or work place, and the opportunity to purchase items from vendors located anywhere in the world. For the online retailer it allows them to reach a potential worldwide market and to build up brand reputation and loyalty in a cost effective way.

However, just as the online shopping environment provides the consumer and retailer with many benefits, it also provides criminals with the opportunities to defraud unsuspecting consumers and retailers, to steal money and to steal financial and personal data. The security concerns arising from this criminal activity could prove to be a barrier to the growth of the online marketplace. According to EUROSTAT's *Internet usage in 2009 - Households and Individuals survey*[1], about one third of the population who have not used the Internet for e-commerce had concerns about payment security and approximately another 30% had privacy and trust concerns.

Addressing these concerns is a key component in ensuring the continuing success of online commerce. While there is an onus on online retailers and merchants to reassure consumers that their systems are secure and comply with the appropriate legal and regulatory environments, there is an onus on consumers to ensure that they conduct their business online in a safe and secure manner.

ENISA believes that a key element for securing the online marketplace is raising users' awareness regarding their privacy, their rights when purchasing items and services online and payment security. This white paper aims to provide a set of recommendations for consumers of the online marketplace so that they are aware of their rights when shopping online and how best to manage and reduce the risk of becoming victims of criminals. In the section, Guidelines for Online Retailers, retailers are provided with an overview of the requirements and obligations they must adhere to when conducting business online to ensure the security of their clients' financial and personal data and fulfilling the contract with the client.

While this document covers a number of the most popular risks and issues surrounding online shopping, it should not be seen as either a comprehensive source of all risks associated with online shopping, or as a technical guideline or specification to secure standards or solutions.

1 EUROSTAT's Internet usage in 2009 - Households and Individuals survey http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-09-046/EN/KS-QA-09-046-EN.PDF

Introduction

Purpose and audience

This report aims to raise awareness and provide practical advice about the risks associated with online shopping for anyone who is engaging in online shopping activities, either as a buyer or seller. It is designed for consumers of all age groups who desire to purchase goods and services online and merchants who offer their goods and services online.

Background

As the use of the Internet has grown, its use as a medium for the sale and purchase of goods and services has grown as well. The broad market available to merchants has made the use of the Internet a valuable tool for established merchants and start-ups alike. Consumers are able to benefit from the wide array of available merchants and goods, the simplicity of comparison shopping between multiple merchants, convenience of shopping at any time, and from any location with Internet access.

Nearly 40% of European Union individuals shopped on-line in 2009, according to EUROSTAT's *Internet usage in 2009 - Households and Individuals survey*[2]. Online shopping is without doubt an ever-increasing global phenomenon. However, the survey also revealed that about one third of the population who had not used the Internet for e-commerce had concerns about payment security and approximately another 30% had privacy and trust concerns.

In this paper we will study the anatomy of online shopping, explore the risks and propose, where possible, countermeasures and advice that can significantly reduce these risks, both for the online customer and online merchant side.

2 EUROSTAT's Internet usage in 2009 - Households and Individuals survey http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-09-046/EN/KS-QA-09-046-EN.PDF

Online shopping

Definition

Online shopping is the ability for people to purchase and/or sell products, or services, over the Internet or using any similar public electronic network.

History

While the Internet has been around for a number of decades, it is only since the early 1990's that it has been widely adopted. Initially developed to share information, the Internet grew rapidly post 1990 after Tim Berners Lee created the first World Wide Web server. This was quickly followed by the release of the first web browsers, which made interacting with the Internet a much more intuitive and easier task for end users. These two innovations resulted in a major growth in the Internet over the following years.

It was not until 1994, when Netscape introduced SSL encryption into their browser, that people started to consider the Internet as a means for conducting transactions in a secure manner.

The first known web purchase took place in 1994 and was for a pepperoni pizza from Pizza Hut. Some of the first e-commerce websites, such as Amazon, which first started trading on July 16th 1995, and eBay have now become major organisations and household names.

In the time since then, e-commerce sites and markets have grown enormously, with consumers able to purchase most items online without leaving the comfort of their home or business.

Evolution and latest developments

Originally, online shopping was confined to buying and selling standard items such as books, CDs, DVDs and other similar items. Over time, the range of goods and services has grown exponentially and now includes food, airline tickets, hotel and holiday bookings, downloadable movies and music, subscription services to online media sites, fragrances and electronic goods; and these are just an example of what is now available online.

In the beginning, online shopping was restricted only to those who could afford access to a computer at home, or had access to one in their workplace. Now with the proliferation of cheaper computers and Internet access, many more people are coming online. In addition, better Internet infrastructure to homes and businesses, such as broadband, is enhancing the experience of people on the Internet and encouraging them to do more online.

This growth and evolution in online shopping is evidenced from many surveys and other research material in this area. In February of 2010, the Centre for Retail Research (CRR)[3] published their "eCommerce and Online Retailing" report, which stated that online retail sales within Europe were likely to grow 19.6% to 172 billion Euros (150 billion pounds) in 2010.

3 Retail Research (CRR), eCommerce and Online Retailing Report http://www.retailresearch.org/onlineretailing.php

The Centre for Retail Research forecast online sales growth would be fastest in Poland, up 36%, followed by France, up 31%, and Spain, up 25%, as they catch up with more mature markets such as Britain, Germany and Nordic countries. Britain, where online retail sales accounted for 9.5% of total sales in 2009, will see the slowest growth, up 12.4%. However, it will remain the largest market, worth an estimated 48 billion Euros. Last year, European online shoppers spent on average €871 each, with Britons topping the table with an average spent of €1,240 and Poland at the bottom of the countries surveyed on €362.

Retail Decisions (ReD), a UK based company specialising in card fraud prevention, payment processing and card issuing, reports that 2009 online retail sales were at an estimated GBP 49.8 billion, up 21% from 2008 as up to thirty-three million consumers hit their computers[4]. Carl Clump, CEO of Retail Decisions commented, "In 2009, 30% of online sales took place in November and December underlining the importance of the holiday season to retailers. The top five busiest days of the year, all Mondays, took place over this period. In the UK, Monday, 7th December was the biggest online shopping day of the year, up 16% on 2008 at an estimated GBP534 million. For the first time in the UK, a post-Christmas Monday, 28th December, made it onto the list of top performing online days."

In their recent "US Online Retail Forecast, 2009 To 2014"[5] the research organisation Forrester highlighted that online retail managed a noteworthy 11% year-over-year growth in 2009. Topping out at $155.2 billion in sales in 2009, 154 million individuals bought online, representing 67% of the online population and a 4% increase in the number of Web buyers over the previous year.

Online retail sales aren't growing at the torrid pace they once were, but they continue to grow steadily. Forrester Research put out a new five-year forecast in March 2010[6] predicting that e-commerce sales in the U.S. will keep growing at a 10% compound annual growth rate through 2014. It forecasts online retail sales in the U.S. will be nearly $250 billion, an increase from $155 billion in 2009. Last year, online retail sales were up 11%, compared to 2.5% for all retail sales.

In Western Europe, Forrester expects a slightly faster 11% growth rate for online retail sales, going from $93 billion (€68 billion) in 2009 to $156 billion (€114.5 billion) in 2014. Forrester's estimates exclude the online sales of automobiles, travel, and prescription drugs.

Some other statistics of note from the U.S. forecast include:

- E-commerce sales will represent 8% of all retail sales in the U.S. by 2014, up from 6% in 2009
- In 2009, 154 million people in the U.S. bought something online, or 67% of the online population (4% more than in 2008). Three product categories (computers, apparel, and consumer electronics) represented more than 44% of online sales ($67.6 billion) in 2009
- While $155 billion worth of consumer goods were bought online last year, a far larger portion of offline sales were influenced by online research. Forrester estimates that $917 billion worth of retail sales last year were "Web-influenced." It also estimates that online and Web-influenced offline sales combined accounted for 42% of total retail sales and that percentage figure will grow to 53% by 2014, when the Web will be influencing $1.4 billion worth of in-store sales

It is clear that the online marketplace provide companies with a platform to better promote their products and services and increase their sales, while at the same time, benefiting the consumer in providing a wider range of vendors with which to do business. Online shopping will no doubt continue to grow from strength to strength over the coming years, as more vendors invest in their online presence and as more buyers gain trust in the services provided.

4 Retail Decisions (ReD) Press Release, 2009 Online Retail Sales Finished An Estimated 21% up From 2008 http://www.redplc.com/81_1430.asp
5 Forrester Group, US Online Retail Forecast, 2009 to 2014 http://www.forrester.com/rb/Research/us_online_retail_forecast%2C_2009_to_2014/q/id/56551/t/2
6 Forrester Group Forecast, Double-Digit Growth For Online Retail In The US And Western Europe http://www.forrester.com/ER/Press/Release/0,1769,1330,00.html

Trends

There is no doubt that the trend for the use of online shopping, both by businesses to sell to consumers and for consumers to sell to each other, will continue to grow. This will be facilitated by the increasing numbers of businesses and people coming online. How people interact with the web is also changing and this will impact the landscape of online shopping. Some of these initiatives will be;

Mobile Internet: More and more people are accessing the Internet from their mobile phones, smartphones, PDAs and tablet devices. Most of these systems, by their nature, are connected to the cellular network and are therefore always connected to the Internet, provided there is sufficient coverage. This means people will no longer be restricted to conducting their online shopping from their computers, but can also do so from their mobile devices. The challenge this will bring will be for sellers to ensure their online services can interact with the current limited browser functionality found on those devices. It will also mean that consumers will also need to be made more aware of the dangers of accessing the Internet from their mobile devices.[7]

Social networks: More and more people are using social networks, such as FaceBook, Twitter and LinkedIn, to name but a few. Social networks are now becoming marketplaces and are facilitating online shopping. This poses a number of issues as, due to their nature, social networks have access to a lot of private information belonging to their members. Should users of the social networks not have their privacy settings correctly configured, they may find themselves targeted by online sellers, offering goods and services aimed specifically at them, based on their private details. As the use of social networks continues to grow, we will no doubt see this as an on-going trend and one that will need to be managed. People should also be aware that criminals often use Social networks to transfer malware to users (sending a message posing as a friend). This can lead to control of the users account and subsequent fraud.

Applications (Apps): Many companies are now providing applications, or apps, to enable customers to access their services. Using an app means the user does not have to access the service or system using a web browser, but can interact over the Internet just using this specific application. A number of online sellers are now providing their own customised apps to allow their customers to directly access their online shop to purchase goods or services. An example of this is Amazon's Kindle app, which allows customers to purchase and download electronic versions of books onto their mobile device. Another example is that a number of grocery stores, such as Tesco in the UK, are now providing customers with an app to enable them conduct their online shopping.

Barriers

As popular as online shopping has become, fears over potential fraud and identity theft still keep millions of consumers from buying goods and services online. The inaugural VeriSign Internet Trust Index Report, published in March 2010, found that one in three frequent Internet users say they're "extremely concerned" about the risks of online shopping.

These consumers avoid shopping online because they simply do not trust it.

Their worries are not unfounded: the same survey found that 11% of the UK's online population reported they had experienced some form of online fraud over the past 12 months. On average, online consumers lost £352 to identity theft during the year, and 12% of fraud victims are still waiting to recoup their losses, while 4% believe they never will. The British aren't alone: 15% of German Internet users say they suffered ID fraud, along with 10% of French users, 9% of Italian online consumers, and 3% of Sweden's online population.

Without the appropriate safeguards, policies and knowledge needed to establish a relationship of trust, the real-world threat of online fraud will continue to exclude significant numbers of consumers from engaging in e-commerce.

7 ENISA Report, Online As Soon As It Happens http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens

Environment and main drivers

There are two main drivers for merchants to enter the online shopping market. First is the potential to access a global market via the Internet. Vendors are able to address a vastly larger audience for their goods or services, as their websites can reach new markets at a fraction of a cost. Indeed, it has been demonstrated that the costs associated with selling goods and services online can be in many cases much less than traditional "bricks-and-mortar" methods, where retailers utilise fixed building locations to sell their goods and services. Online shopping eliminates much of the sales floor overhead, such as sales personnel (and associated turnover), display materials and multiple fixed locations that lack the flexibility to change as the market changes. This flexibility is also an advantage to smaller or start-up merchants, who often lack the capital to invest in "bricks-and-mortar" retail models, but who can vastly increase their market exposure through an online presence. Customers can benefit from the wide array of available goods and services with increased competition.

The online shopping environment is made up of a number of elements, primarily;

- Online merchants
- Bank and payment services
- Internet infrastructure services
- Regulators
- Technology

Online merchants

Online Merchants fall into several categories. A brief analysis of each category follows:

Manufacturers

Some merchants are original manufacturers of goods and service,s who choose to market their products using the Internet in order to simplify the sales process and costs associated with a direct sales force, or the costs associated with "bricks-and-mortar". The site offers the possibility for these merchants to present their goods alongside marketing and product literature that can position the products in a manner that matches customers` perceived needs. This allows the manufacturer to keep a great deal of control over the marketing and positioning of their products. These merchants offer the goods that they manufacture, and may also provide information on how the consumer can buy these products through other sources. The online shopping site will offer payment services to allow the consumer to input their financial information in order to complete the sale and shipping services for the delivery of the products. The manufacturer may also offer product registration for purchased products and support information, as well as warranty repair services.

Retailers

Some merchants are either existing or new retailers, who discover the potential cost savings, market exposure, and marketing advantages that an online shopping and marketing presence creates. These retailers market a variety of goods that are similar to those you might find in a traditional retail establishment. They offer several types of goods and may also present competing products and manufacturers side by side. This allows the retailer to promote themselves as a useful location for comparison shopping, and as a one-stop shop for their customers.

The retail company can also market their brand image and capabilities through their online site. The online shopping site usually offers payment services to allow the consumer to input their financial information in order to complete the sale, and it will also offer shipping services for the delivery of the products. The retail company may also include additional services, as well as links to the various manufacturers they represent.

Individuals and SMEs

Some merchants are individuals or small companies who participate in online shopping, or auction communities where goods and services are offered collectively through a single website. This method has been popularised by the auction site eBay. On these types of online shopping sites, products can be compared against each other and individual items can be either bid upon or purchased immediately. The website offers additional services, such as verified payment services, purchase insurance, shipping estimation tools, and other added services that can benefit both the merchant and the consumer. This can develop into a highly symbiotic online relationship, with high volumes of repeated sales and increased customer loyalty, whereby the sellers and the buyers also build their reputation record.

Online market places

Should companies not wish to devote time and resources to developing their own online e-commerce presence, they can still avail themselves of the advantages of online selling by indirectly engaging in a number of online marketplaces. These services provide a virtual online marketplace, allowing consumers to shop for items and have a number of companies providing them with pricing on the item they are looking for. The consumer can then select their preferred supplier and have the transaction facilitated by the online marketplace. These marketplaces are quite popular, as they provide companies with a cost effective way to sell their products online, while also offering the consumer a range of suppliers to choose from to which they otherwise might not have access. Some of the more popular online marketplaces include eBay www.ebay.com, Amazon Marketplace http://www.amazon.com/marketplace and others targeted at particular market segments.

Hybrid services

Recently, a hybrid approach to online shopping has appeared, which allows the consumer to perform their shopping online, at the completion of their purchase they can travel to a physical retail store and pick up their purchase.

Consumer to Consumer market space

A growing trend is the use of Consumer to Consumer (C2C) marketplaces. This marketplace allows individuals to sell goods or items they no longer wish to own via an online marketplace. The most popular of these sites is eBay (www.ebay.com), which enables individuals to buy from and sell goods to each other, all over the world. Other sites are also growing in this area, with the bigger online retailers providing consumers with the ability to sell old and unwanted goods. An example of this is the online website Amazon.com. Traditionally associated with selling books over the Internet, Amazon has expanded its product portfolio to include selling other items, such as electronics, DVDs and clothes. It also provides individuals with the ability to sell their used or unwanted books and other items for which they do not have use.

Internet retailers

Internet retailers enjoy advantages that are difficult, or impossible, for "bricks-and-mortar merchants" to realise. Internet retailers can:

- More easily offer a far greater selection of goods
- Avoid the burden of maintaining physical storefronts, so they can pass their reduced overhead costs onto consumers in the form of lower prices
- Enable customers to shop anytime, 365 days a year
- Frequently offer low-cost or no-cost shipping, further adding to the convenience of shopping online

Those advantages are making a difference. In the UK's Royal Mail Home Shopping Tracker 2009, it was found that many UK workers are even opting out of the traditional Friday lunchtime pub outing in favour of spending time shopping online.

It is little surprise, then, that Internet retailers are looking for ways to capture that growing customer base by more effectively differentiating themselves in a crowded, increasingly commoditised online marketplace. In addition to traditional methods – for example, lower prices or unique product offerings - many online retailers are implementing security and authentication safeguards designed to establish trust with consumers wishing to purchase online.

Banks and payment services

There are lots of different ways to pay for online purchases. The following is a brief overview of the more common payment services:

A basic categorisation would be:

- Payment in advance: Complete amount is paid in advance for goods and services. Payment could be done via ordinary bank transfer or, for example, prepaid services such as www.paysafecard.com
- Invoice: Buyer must pay the dealer, according to payment terms in maximum number of days. Payment can take place via bank transfer, cheque, credit card or other payment methods
- Cash on Delivery (COD): Goods are paid for immediately they are received by the buyer, e.g. pay directly the delivery service, as in fig. 1
- Debit note: Amount will be charged directly to bank account.
- Credit card payment: Amount will be charged to the buyer's credit card
- E-Payment
  - Mail-based, like PayPal or MoneyBookers
  - Mobile-phone based systems, like Crandy or mpass.
  - Others, like ClickandBuy or Web.Cent

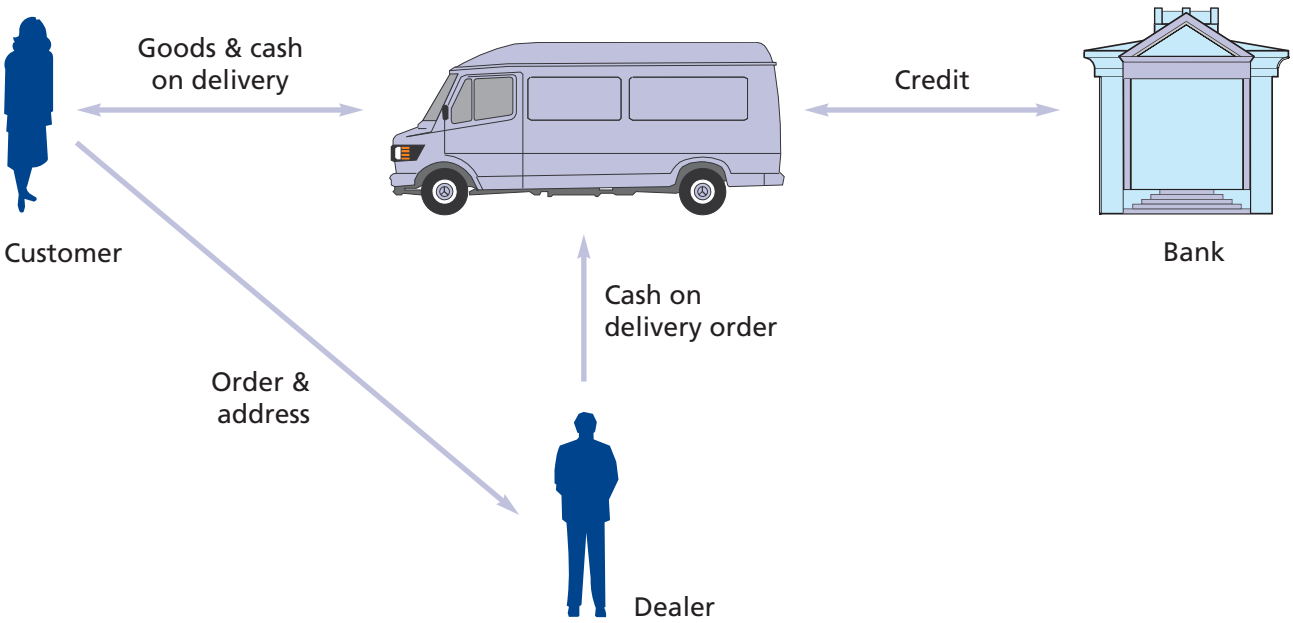

Fig. 1: Process cycle of cash on delivery payment procedures.

Banks

The banking ecosystem is made up of several key actors, who perform financial transactions. From a generic perspective, a bank is a financial intermediary whose core activity is to provide loans to borrowers and to collect deposits from savers.

Payment services offered by banks allow consumers and corporate customers to exchange funds, borrow money and perform other financial transaction services. They cover cheques, credit transfers and may involve depositing funds for a set period of time for a pre-determined or variable rate of interest. Banks offer an extensive range of such savings products, from standard fixed term and fixed deposit rate to variable term with variable rates. They often offer a combination of time and current accounts, whereby customers can withdraw their funds instantly or at short notice (at lower interest rate). In addition, they include standing orders, direct debits, and plastic cards, including debit and credit cards.

It is worth noting that in many jurisdictions, especially within the EU, the banking environment is subject to multiple legal and regulatory frameworks. These frameworks are aimed at protecting personal information pertaining to persons or businesses that use banking services. They include personal data protected under applicable data protection regimes such as the EU Data Protection Directive 1995 and Member States data protection Act(s), financial services government initiatives such as the UK Financial Services Authority, as well as global industry mandates such as the Payment Card Data Security Standard (PCI DSS), the Payment Application Data Security Standard (PA-DSS) and PTS (PIN Transaction Security).

It is also very important to understand that banking and Payment services have become an integral part of national, European and global critical infrastructure. This infrastructure relies heavily on telecommunication "backbones", such as the Internet, as well as on other private transfer services, which are required for national and international banking and online services to work. Without this critical infrastructure in place, there would not be any online shopping and international business would be deeply hindered. Unfortunately, criminals have understood that there are vulnerabilities in both the banking/payment services structure and in the critical infrastructure that supports it.

Credit card payments

Many websites allow people to purchase goods and services by using a credit card. In order to process a credit card payment, websites can accept them in two ways;

A merchant account: This is a facility provided to the website owner by their bank. The requirements for this will vary from country to country and from bank to bank. There is a charge for such a service, which is normally broken down into an initial setup charge and then a transaction fee for each transaction processed.

Third Party Merchant: Otherwise known as payment gateways, Third Party Merchants enables websites to process credit card payments by using the infrastructure of the Third Party Merchant. This means the website owner does not need to be as concerned in setting up and managing their payment facilities, as this is managed by the Third Party Merchant. Normally, there is no set up fee for this service, but there are higher transaction fees.

Wire transfer

Another payment method is to use a wire transfer service to send money to a vendor in return for their goods. Companies providing these services include West Union and MoneyGram, amongst others. One of the disadvantages of this type of service is its vulnerability to abuse for fraudulent purposes.

Payment services

A number of payment services allow people to conduct online transactions without the need for a credit card. People set up an account with the service and can then transfer money into that account to use for the purchase items or services online. People can also use their payment service accounts to receive money, for example if they sell items on an online auction site and someone wishes to transfer money to them. Money from their payment service account can be transferred from their account to their bank account, should they wish to do so. Common service providers in this area include PayPal and Google Checkout

Vouchers

Some sites will sell electronic vouchers that people can use to purchase items on a particular online shopping website. This is normally done by the individual setting up an account with the website and then the value of the voucher is credited against that account. As the account holder buys items from the website, their voucher balance is reduced accordingly.

Internet infrastructure services

Without a reliable and secure Internet infrastructure behind them, merchants would not be able to provide the kind of online shopping experience today's consumers expect and demand. A sound global infrastructure is crucial for shoppers to navigate online and to purchase items safely and securely. It also protects merchants against service disruptions and cyber-attacks, which can result in substantial loss in revenue and rapid erosion of their brands.

Domain Name System (DNS)

A key element of the Internet infrastructure is the Domain Name System (DNS). The DNS infrastructure is used every time an Internet user clicks on a Web page, conducts a transaction, or sends an email, and it is growing quickly. The DNS servers provide the user with the information needed to contact the website they are looking for, similar to the way in which a phone book provides you with the information needed to telephone someone.

Certificate Authorities

Identifying and establishing trust in a retailer in the real world is relatively straight forward. They will most likely be located in a physical building and you can visually verify that what they sell is real. In the online world, however, it is not so easy to establish the same level of trust. All you have to base your judgement on is what is displayed on your computer.

Certificate Authorities (CA) attempt to address the online trust problem by issuing what is known as a digital certificate to the vendor or owner of the website. In order to get a digital certificate, the owner of the website needs to provide the issuing Certificate Authority with documentary proof that they are entitled to be issued with the certificate.

Once a certificate has been issued to a website owner, they can install it onto their website. Most modern browsers will be configured to trust the certificates issued by a Certificate Authority. Therefore when you visit the vendor's website your browser will automatically confirm that the certificate on the website has been issued by the appropriate Certificate Authority.

Internet Service Providers

Internet Service Providers are companies that provide other companies and individuals with the infrastructure necessary to access the Internet. This infrastructure can be in the form of leased lines, broadband access, wireless access or dial-up solutions. The ISP will also assign companies with the appropriate internet (IP) address(es) to enable them connect to the internet and for customers and companies to connect to them.

Top-Level Domain Registry

The domain names of websites are made up of two parts, the name of the site and the domain to which the website belongs which is normally the last part of the domain name. The allocation of names within a certain domain is governed by rules and policies. These are managed by what are known as a Top-Level Domain Registry. Organisations responsible for the management of the Top-level domains are authorised to do so by the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN also operates the Internet Assigned Numbers Authority (IANA) and is in charge of maintaining the DNS root zone.

Internet Registrars

An Internet Registrar, also known as a Domain Name Registrar, is an organisation that has been accredited by a top-level domain registry or by a country code top-level domain, to manage the allocation of domain names for websites. The registrar will issue domain names in accordance with the rules and policies associated with the domain name extension.

National regulators

Online shops are a key element of today's virtual world, a world without borders providing information society services, as well as being part of it. National regulators are central agents for guaranteeing transparency of the business operating upon the Internet and to give confidence to citizens while they shop online. The main tasks of the regulators are:

- To establish regulations and to give instructions on practices to be followed
- To monitor compliance with the rules on electronic commerce
- To order the opening of breach proceedings and to carry out the respective investigation, as well as to apply the sanctions provided for
- To determine the suspension of the activity of service providers in view of serious irregularities and on grounds of urgency
- To publish online the most significant codes of conduct of which they have knowledge
- To publish other information, namely court decisions within this field
- To cooperate nationally and with other European Regulators

For the purposes of this paper, the regulators of most concern are those identified as having jurisdiction over electronic commerce. Typically these are:

- Data protection authorities
- Consumer protection authorities
- Communications regulators.

Data protection authorities

Each member state of the European Union must have the appropriate regulator in place to ensure that the EU Data Protection Directive 95/46/EC is implemented and enforced. The Data Protection Directive ensures that organisations should respect the individual's right to privacy when conducting business with them.

Consumer protection authorities

Most member states have a consumer protection authority to defend the interests of consumers, enforce consumer related laws and promote a robust consumer culture. Consumers with issues relating to retailers or other providers can refer their problems to the consumer agency, which can investigate further. As well as ensuring local consumer protection laws are upheld, the consumer protection authority is also responsible for ensuring that companies abide by the EU Electronic Commerce Directive.

Communications regulators

One of the concerns many consumers have when shopping online is that they may be subjected to continuous and unwanted emails from the selling organisation. In 2002, the EU introduced the Electronic Privacy Directive, which outlines the privacy rights of individuals and how companies should contact them via electronic means, such as email, mobile text messages or by phone calls. This directive in effect prevents organisations from contacting individuals by those means, unless the individual has given explicit permission for them to do so.

Risks related to shopping and paying online

It is much harder to determine who you are dealing with online and the processes for obtaining the goods or services you need, compared to the physical world. Therefore, it is important to ensure that you consider the overall risks to your Internet activities and control them to a level with which you personally feel comfortable.

The Internet has enabled criminals to improve and expand their activities just as readily as it has allowed the same for consumers and legitimate merchants. The advantages of international exposure, low transaction costs and rapid communications have allowed many traditional crimes a new lease of life and have enabled a few new ones. The increased problems in complaining effectively across languages and legal jurisdictions also help to shield criminals from some of the consequences of their actions.

Fraud, generally, is profiting by deception and is a continual problem on the Internet, driven by the low costs of email and web hosting. There are many different aspects of fraud online – fake shopping and banking sites, criminals looking to copy your access credentials to financial and other websites, malicious code and non-receipt of goods.

Online fraud

When we talk about 'online' fraud we refer to any fraud that is perpetrated using online services such as email, messaging applications or websites.

The most common forms of online or Internet fraud include:

- Phishing
- Spyware
- Internet scams, such as so-called '419' fraud
- Overpayment scams
- Man in the Middle based fraud attacks
- Man in the Browser based fraud attacks

However it is worth noting that some elements of the fight against specific types of fraud are improving. Efforts to educate customers about the threat posed by phishing and spyware are paying off, with customers becoming more security aware. Banks have also been increasingly successful in detecting and preventing suspicious transactions. Another factor for some banks has been the introduction of stronger methods of authenticating customers, such as the 'chip and PIN at home' devices introduced in the last few years.

Phishing

One of the most common techniques used by fraudsters to obtain an individual's sensitive information, such as their financial details, is phishing, whereby a bogus organisation is set up purely to obtain valuable personal information.

For example, you may receive an email that purports to come from your bank. The email may request that you send the "bank" your account details, as they are updating their database. You click on a link in the email to what you think is the bank's website, but instead the link takes you to the fraudster's website. You proceed to enter your account information.

The fraudster now has all the information he needs to use your identity to conduct illegal transactions.

There is a wide variety of goods and services being advertised on underground economy servers, and many of these goods and services form a self-sustaining marketplace.

Spam and phishing attempts are attractive, because of their effectiveness in harvesting credit card information and financial accounts credentials.

Spyware

Spyware is a type of computer virus that can be installed on your computer without your knowledge. Spyware is sometimes capable of acting as a 'keystroke logger', capturing all of the keystrokes entered into a computer keyboard. Typically, the fraudsters will send out emails at random, to get people to click on a link from the email and visit a malicious website, where vulnerabilities on the customer's computer are exploited to install the spyware.

The emails are not normally related to Internet banking or ecommerce sites, and try to dupe people into visiting, or clicking on the link to, the malicious website, using a variety of excuses.

The spyware will then monitor all keystrokes and activity on the computer and send information such as banking credentials, credit card details, user-ids and passwords for websites to the criminals without you being aware of the activity.

Advanced Fee fraud

For years, consumers across the globe have been receiving suspicious letters or faxes from unknown persons asking for financial assistance or announcing that the consumer had unexpectedly come into a financial windfall.

Many of these frauds originate in Nigeria and usually involve a plea or demand for funds up front in order to receive the "promise" of "good" money that the customer has won or deserved.

Due to the feature of having to pay up front, these types of scams are sometimes referred to as "Advanced Fee" scams or "419" scams, named after the Nigerian Criminal Code that prohibits the activity of receiving property under false pretences.

These frauds have diversified and adapted over the years and now take many different forms. The end result certainly remains the same, that is to trick the unsuspecting consumer out of billions of dollars, euros, etc.

There is a number of variants of the scheme, including:

- Fake lottery winnings – for lotteries into which the victim didn't realise they had been entered. For some reason, a lot of these reference Dutch lotteries, although the famous Spanish "el Gordo" lottery is also used
- Taxation refunds – false promises of tax refunds may be advanced-fee fraud, although they can also be phishing attacks
- Untraced legacies – a crooked banker or lawyer offers to share a large unclaimed inheritance if the victim pretends to be the next of kin
- Stolen funds – the alleged profits from some crime or recovered stolen funds, such as a recent variant of this scam relating to US soldiers returning from Iraq, will be shared with the victim if they allow the funds to be transferred via their bank account
- Most humorously, one was issued claiming to be looking for money to return a Nigerian astronaut from a secret Russian space station[8].

Needless to say, all of these are false although the fraudsters have a comprehensive arsenal of tricks to convince people that the money really exists, such as fake documentation, false bank websites and even exact copies of legitimate bank sites.

Overpayment scam

In this scenario, the victim is selling something such as a computer, or other high value item, on the Internet using one of the Consumer to Consumer websites. Once they have posted the item online, they begin to receive numerous inquiries from overseas.

8 The Register – Cosmic 419er Lost In Space - http://www.theregister.co.uk/2004/04/16/cosmic_419er/, April 2004.

The victim is excited that someone is interested in purchasing the item and agrees to sell it to the buyer. The buyer intentionally sends a cheque, or bank draft, that is for more than the amount for which they are supposed to be buying the item. The victim agrees to send the buyer a cheque for the difference. Several days later the victim discovers that the cheque is falsified and it is returned, resulting in the victim not only losing their high value item but also losing the money they sent to the criminal.

Man in the Middle attack

A 'Man in the Middle' attack is a form of attack in which an unscrupulous third party intercepts communications between two computers. The third party captures the data, but still relays it to the intended destination to avoid detection. This can allow the attacker to intercept communications on a secure or encrypted channel.

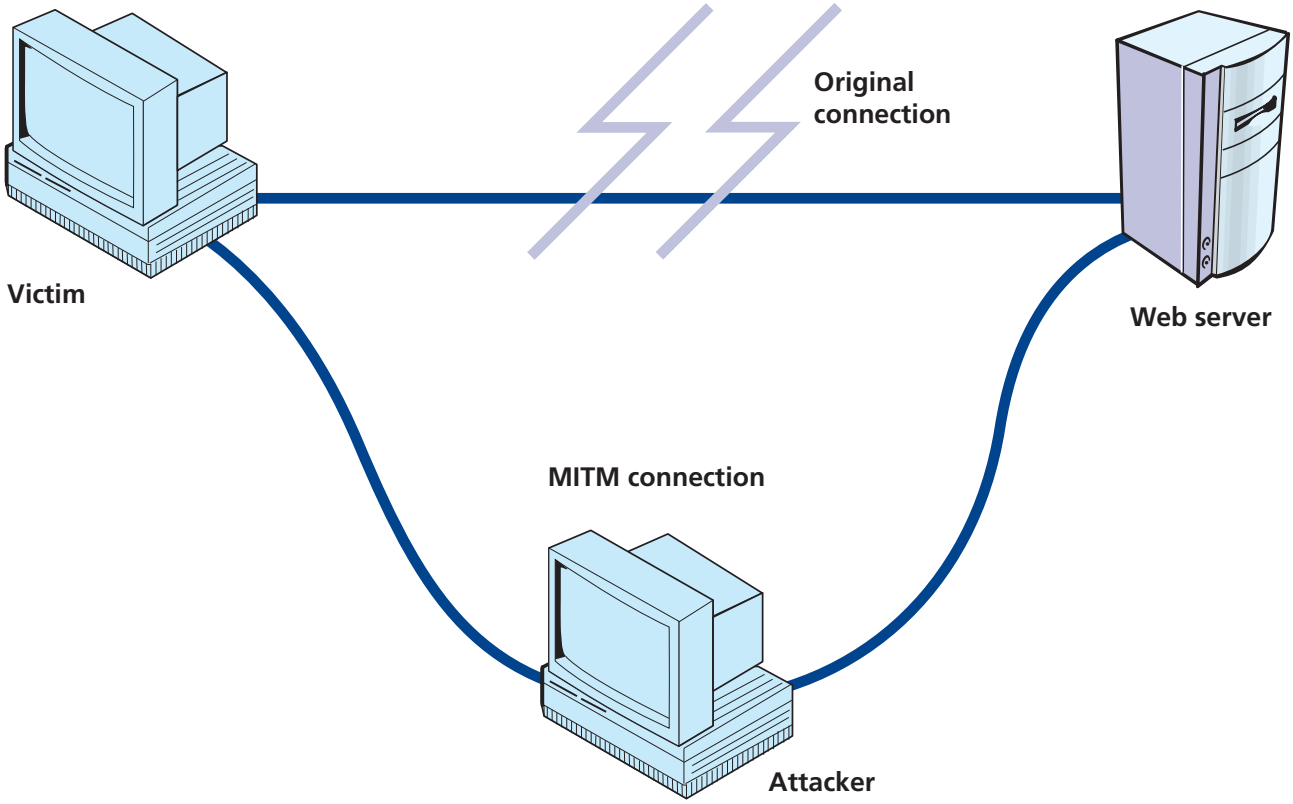

Fig. 2: Overview of the Man in the Middle attack

Man in the Browser attack

In a 'Man in the Browser' attack the perpetrator installs a Trojan horse on a victim's computer, which is capable of modifying that user's Web transactions as they occur in real time. An example would be the Zeus Trojan, which is designed to intercept secure traffic from the infected PC to the victim's bank's website and display false information to give the victim the impression their account has not been compromised.[9]

"Compromised" sites

Not all sites used for fraud are themselves fraudulent – many legitimate sites have found themselves compromised by attacks on their web-servers, or service providers and have been used to compromise visitors. This can often happen through the compromise of a third party component on the web site – such as Flash components, an advertisement provider or by compromise of the hosting company service.

9 Atif Mushaq, Man in the Browser: Inside the Zeus Trojan, Threatpost 19th February 2010 http://threatpost.com/en_us/blogs/man-browser-inside-zeus-trojan-021910

Criminals will then install malicious software on the compromised website to infect the PCs of those visiting the site. The purpose of this malicious software will often be to compromise the victim's sensitive data. Other uses criminals have for compromised sites is to redirect the visitors to the criminals' own fraudulent site in order to defraud the visitor.

Even when visiting well-known sites, visitors to the site need to be wary of warnings from anti-virus products or browsers about malicious or suspicious content.

Vulnerabilities in or related to installed software

The software you use, whether it is part of the operating system, an Internet browser or utility software, may have vulnerabilities, which a fraudster can attempt to exploit. It is essential that you try to keep software up to date.

Most software manufacturers or vendors will provide an alerting service and an automated patch or update facility and, if possible, you should make sure these are active. Even if a security flaw is not being actively exploited when the correction is released, criminals are normally able to use the new code, through a technique known as "reverse engineering", to produce an effective exploit. This will often be used in online attacks on the same day as the correction is released.

Fraudulent e-commerce sites

Often the fraudulent e-commerce websites are based on the selling of technology goods with a very cheap price, or some "grey market" items like prescription medication, tax free items, music, movies or other similar items. This scam can have two main goals:

Steal payments: Many bogus e-commerce sites require advanced payments, using money transfer services such as Western Union or Money Gram. This allows the scammer to immediately cash out your payment, while the goods will obviously never be shipped. Scammers are inclined to use excuses like "the packages were lost, we dispatched them again", "the item you purchased is currently out of stock" or similar. This behaviour allows the scammer to diminish the users' complaints and extend the life of the bogus e-commerce site.

Stealing credit card information: Fake e-commerce sites are set up on free hosting servers and their existence is usually spread with the use of spam emails. Very often when victims visit the site and complete a transaction, they get messages ranging from "OK, transaction completed, the goods are being shipped" to a "there was an error with your credit card/our payment system". For the criminal, what really counts is having few days before the buyer becomes suspicious and alerts their credit card issuer to a possible fraud.

The bogus web site's life is normally quite short. Yet, despite this kind of fraud being easily recognisable, the scammer can collect a large number of credit card details, depending on the quality of the spam email and web site style.

The stolen credit card details will usually then be sold on via the criminal underground marketplace until they reach the last link in the chain. These criminals will then use the credit card information to buy real goods online, or convert it to "electronic gold".

Auction site fraud

While the online auction market is not as affected by organised crime, the amount of defrauded money grows day by day. Common methods of fraud can be quickly summarised:

- Misleading goods description: This fraud is based on using language-specific tricks to deceive the buyer into thinking that they are about to purchase what they want, although this is not the case. A clear example could be the advertising for a new 32 Gb IPhone for a very cheap price, whereas the actual item being auctioned is something completely different

- Fake auction from a stolen account: This is a particular kind of ID theft, where organised criminals buy the credentials for a real seller on a particular auction site from the underground marketplace, in order to take advantage of their good feedback. They then change the payment method and start to sell goods at a lower price than the usual price. The payment method is usually changed to a system that allows for the easy and fast transfer of cash, such as Western Union or MoneyGram services

Spamming

There are several definitions of spam, however it is accepted that all of them have the following characteristics in common:

- Unsolicited messages, where the recipient has not granted verifiable permission for the message to be sent
- Sent in "bulk" or as part of a larger collection of messages, all having substantively identical content
- Often has a commercial purpose
- Sent by different means of electronic communications (namely through automatic calling machines, facsimile machines or electronic mail) and able to be stored in the network, or in the recipient's terminal equipment until it is collected by the recipient
- Spamming by electronic mail, commonly using addresses obtained without owner's permission
- This is often illegal, misleading and/or harmful
- Often sent by someone using a false identity

Unsolicited communications for marketing purposes aren't just junk messages. Nowadays fraud and crime are a concern commonly associated with spam. Examples of this could be:

- Phishing – fake websites that seem to be genuine. The purpose is to harvest confidential user data, identity fraud and cause damage to companies' reputations
- Spyware by e-mail or through software to track and report a user's on-line behaviour
- Spyware may also collect personal information, such as passwords and credit card numbers
- The spread of malicious codes, such as worms and viruses. Once installed, they allow an attacker to take control of an infected computer system and turn it into a 'botnet', hiding the identity of the real spammer. A botnet is a network of compromised machines that, without the knowledge of their owners, are under the control of criminals and are then used to commit crimes, such as sending spam, attacking other computers or extorting websites

Identity theft

Identity theft occurs when a criminal tries to assume someone else's identity for the purpose to obtaining benefits and eventually charging the cost to the victim. This information is often collected by criminals using phishing attacks, installing spyware on their computers, gathering information via fraudulent websites or simply gathering the data from people's profiles on social networking sites.

There are several reasons that can attract criminals to commit ID theft, some of which are:

- Creating a bank account and requesting a credit/debit card, which will then be used to fraudulently purchase goods and withdraw money from an ATM
- Creating virtual money accounts on sites like PayPal, MoneyGram, Western Union or Liberty Reserve. These accounts will be used to collect money gained from other criminal activity such as credit card number selling, fraudulent activity on auction sites or money stolen from bank accounts
- Creating "real" profiles for clandestine immigrants and selling them genuine identity cards to enable them to live legally within that state

Identity theft has been classed as one of the most rapidly growing crimes.

Completion issues

A particular issue with distance selling of all sorts and particularly Internet sales is the completion of the sale. Customers should receive goods in a proper condition (as new or otherwise as described on the sale particulars), in proper time and fit for purpose.

If you do not receive the goods or if you receive something other than you expected, your initial point of contact should be with the vendor because it is their legal responsibility to correct any error. The vendor will also have the contract, including any insurance rights, with the courier or postal service. Therefore, they should also attempt to sort out a wrong delivery address, or similar issues.

In the event that the vendor refuses to resolve any issue, you may be able to claim a refund through your payments service. Should that fail and the vendor is located within the European Union, you should contact your national consumer protection agency and report the issue to them. You may also be able to address completion issues through your payments service provider.

Mechanisms in place to combat threats

European Directives

Within Europe and relating to shopping online, or put simply, e-commerce, there are three main Directives. In chronological order these are:

1. The Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts.
2. The Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer good and associated guarantees.
3. The Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

These Directives are focused more on e-commerce and defining the differences between business to consumer (B2C), business to business (B2B) and consumer to consumer (C2C).

European Directives have legal effects at European level as part of Community law, but each Member State has to implement the Directive within its national legal framework. Furthermore, it is important to remember that these Directives contribute to the composition of Community law and, due to their effects, they are applicable in the case of disputes among European citizens.

The most important Directive relating to e-commerce is the Directive 2000/31/EC. This says what information has to be provided by the service provider (article 10) “clearly, comprehensibly and unambiguously prior to the order being placed by the recipient of the service”.

Moreover, after placing the order, “in cases where the recipient of the service places his order through technological means, the following principles apply: a) the service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means; b) the order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them” (article 11).

Hence, to summarise, the Directive 2000/31/EC provides the protection of consumers’ interests during the phases of the shopping online process.

National legislation in place by country

The Directives are part of the European legislation system and are addressed to the Member States for alignment with their national legislation.

It is important to note though that both the European Directives and national laws of Member States only apply to websites operating from within the European Union, or in the case of national law within that country's jurisdiction. Therefore, consumers purchasing goods from websites not governed by European law will not have the same levels of protection as if they were purchasing from an e-commerce site within the European Union.

Compliance regimes

Online merchants and the payments services industry are aware of the online activities of criminals, as they have had to deal with the complaints and the financial losses over the past decades. As part of their defences, there are a number of compliance regimes in place to assist in maintaining secure online sites and helping you to recognise which sites have appropriate security.

PCI-DSS

The Payments Card Industry Security Standards Council was set up by the main Credit Cards Industry bodies – MasterCard, Visa and Discover – to promulgate a minimum standard of security controls applicable to online merchants. The "Data Security Standard" – PCI-DSS – was initially released in December 2004.

With version 2.0 of the standard currently in force and a 2-year revision programme, most online merchants – enforced by the financial organisation acting as their merchant acquirer – should now adhere to PCI-DSS. However, as a consumer, you will not find any indication on a website whether or not they are compliant with the standard.

PCI DSS applies to any entity processing, transmitting or storing credit cardholder data. As such it typically applies to merchants of all sizes, from corner shops to multi-national retail organisations, payment service providers and gateways, as well as acquiring banks.

In terms of PCI DSS, there are four levels for merchants:

- The most onerous level is level 1, for merchants with over 6 million credit card transactions annually
- Level 2, for merchants with between 1 million and 6 million credit card transactions annually
- Level 3, for merchants with between 20,000 and 1 million credit card transactions annually
- Level 4, for merchants with fewer than 20,000 credit card transactions annually

The transaction count covers all type of transactions, whether through point of sale devices, e-commerce or phone/mail order. The level that applies to a vendor will determine what levels of scrutiny it must adhere to;

- Level 1 merchants must be assessed annually by a Qualified Security Assessor and must perform a quarterly scan of their external facing IPs linked to the cardholder data environment.
- Level 2 merchants need to complete a Self-Assessment Questionnaire and quarterly scans.
- Level 3 merchants need to complete a Self-Assessment Questionnaire and quarterly scans.
- Level 4 merchants need to complete a Self-Assessment Questionnaire and quarterly scans.

Scans have to be performed by an Approved Scanning Vendor (ASV) and Self-Assessment Questionnaires are typically sent to the acquiring banks, or payments service providers, who then report on their merchants' compliance to the credit card brands. However, please note that some validation requirements vary by country and by brand. Check directly with your brand for full information. The following site also offers guidance on validation mechanisms for all brands: https://www.pcisecuritystandards.org/qsa_asv/index.shtml

Consequences of non-compliance with PCI DSS
If merchants are breached, they are automatically moved up to level 1, which means that they will have to have an onsite QSA audit every year, notwithstanding having to have a forensic investigation and the fact that they will more than likely have to pay legal fees.

Additional items for consideration by merchants are as follows:
- Increase in fraud levels
- Harm to your business
- Card re-issuance costs (costs passed to the merchant)
- Fines that might be imposed on your business by the brands and by banks
- Inconvenience to customer and loss of consumer confidence
- Adverse publicity for your organisation
- Name and shame
- Brand and reputation damage
- Legislative interest – threat of governmental regulation

"Safe Site" badges
Additionally, there are a number of commercial regimes that claim to provide some degree of assurance of web-site security. Some of these merely mean that the site uses a particular vendor, which may or may not give any indication of actual or potential security. Others provide basic security services, such as daily security scans for malicious code, or online security vulnerability assessment. Most security experts are sceptical about the effectiveness of these schemes and would suggest that you neither rely on them if you are suspicious of a site, nor refuse to purchase from a site because it lacks a logo. The world's largest online merchant, Amazon, for example, does not use any of these certifications.

SSL
"Secure Sockets Layer" and its replacement version "Transport Layer Security" (TLS) are encryption techniques designed, amongst other things, to protect the communication between your computer and a website. They also provide a degree of authentication of a website – in that the digital certificate issued should contain the "Fully Qualified Domain Name" of the computer providing the web content.

You should be aware that it neither provides any security to your computer nor does it indicate any level of security implemented at the website – the protection is purely to the communications channel between the two computers. In effect, this acts as a private channel between your computer and that of the website, which only the two of you can access. You should be able to recognise when SSL is being used: the address of a website will begin 'https' rather than 'http' and most browsers will display an icon of a locked padlock, often close to the website address. Many modern browsers will also have other features – the address box may turn green, for example – learn to recognise the indications your favourite browser provides.

Fig. 3: SSL sites displayed in Mozilla Firefox 3.0 and Microsoft Internet Explorer 7.0

Regardless, you should be aware of the information provided by the certificate – and any certificate warnings that your browser gives you. Any competent computer administrator can easily create valid SSL certificates, therefore browsers conduct a degree of checking designed to give you a basic level of assurance. Generally, a browser will check that the certificate has been issued by one of the well-known "Certification Authorities", such as VeriSign or Entrust, that the FQDN for the website matches that of the certificate and that the certificate is in date.

A reasonably common failing of even quite large merchants is to forget to renew a certificate, but if the browser generates a certificate warning, you should consider it a strong indication of increased risk. Browsers will also allow you to view more detailed information associated with the certificate – normally by clicking on the padlock icon.

Most modern browsers will allow you to display a "Verified by" or "Certified by" message. For Windows Explorer, you may select the lock icon to the right of the URL window, as shown in Figure 4.

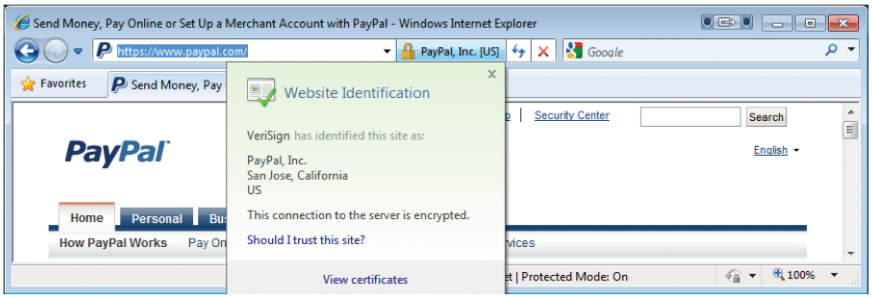

Fig. 4: Website verification in Microsoft Internet Explorer 7.0

With Firefox, you may select the security information area to the left of the URL window, as shown in Figure 5.

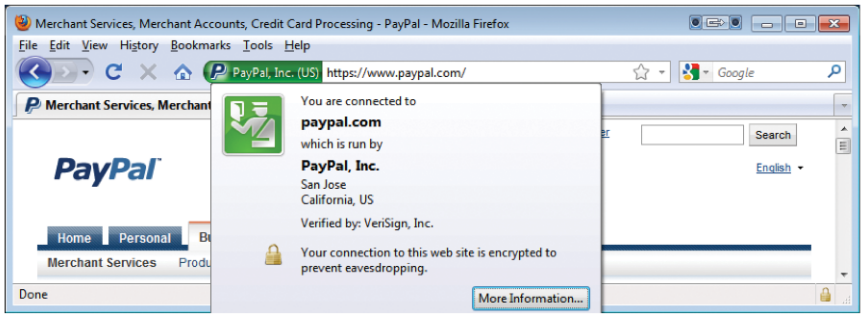

Fig. 5: Website verification in Mozilla Firefox 3.0

You can then check to see if the information in the certificate matches the organisation you are doing business with. This information can be verified in the same windows as above, or you may also click on the "Details" or "More Information" links to view more details about the certificate of the site.

Should you be accessing a website across an insecure or unencrypted link, i.e. not using SSL, be careful when submitting any sensitive information, whether it be personal or financial. Any website asking you to provide such information without providing this basic and cheap protection is likely to be missing other, more critical security controls.

Strong authentication

Multi-factor authentication, a form of strong authentication, combines two or more of the following forms of authentication:

- Something the user knows (ie: their username and password, their PIN)
- Something the user is (ie: biometric data, such as retina patterns or a fingerprint)
- Something the user has (ie: a card or a token)

Requiring several forms of authentication makes it difficult for identity thieves to impersonate someone. The method of combining several forms of authentication is used to verify an identity in a transaction with a high degree of confidence. One of the most common applications of multifactor authentication is using a card to execute operations in an ATM. A variety of credentials are available that suit the end user, from small, credit-card shaped tokens to a mobile application that consumers can download for free.

Guidelines to consumers

When it comes to staying safe online, prevention is far better than the cure. Consumers need to remain vigilant at all times. But it isn't as difficult as it may sound. The following are a few tips that every consumer can keep in mind before they go online and while they're shopping.

Protect your privacy

Identity thieves only need a few pieces of information about you to gain access to accounts, or establish lines of credit in your name. In some cases, they may not directly use the information they gather; rather, they'll sell it on the black market, which can make it much more difficult for you to determine how, when, or where they captured it.

That's why it's vital to follow these tips to protect your privacy:

- It's important to check an online merchant's privacy policy to understand how the company handles information it gathers about you. If you don't like what you see, shop elsewhere
- Don't share passwords, ever. And change them every six months or more often
- When you do choose a password, use a mixture of letters (both upper and lower case), symbols and numbers in combinations that cannot be easily guessed. The longer, more complex the password, the harder it will be to crack
- Use strong authentication wherever you can. A fraudster may be able to uncover your sign-on and password, but he isn't likely to have possession of your credential (token, card or mobile phone) that generates the security code you need to achieve strong authentication. In other words, don't rely solely on your password to protect your data but use additional authentication facilities where available, such as tokens, smartcard, or in some cases services that use mobile phones to send you a one-time pin by SMS.
- Always check the privacy settings on social media and communications applications. Enable maximum privacy as a default – you can always reduce it for individual posts
- Be careful who you befriend – anybody can set up an account in any name on most social networking sites
- Think very carefully before publishing any information that would be used by companies and organisations to verify your identity – especially birth date and location and mother's maiden name
- When you are asked to complete online forms, think carefully whether the organisation really needs to know the answers, as long as you remember them
- When entering your data into a website, remember that it is not necessary to input all the data requested. Only enter the information necessary to conclude the transaction, such as name, surname, email address, delivery address. It is advisable not to input other data to avoid marketing, advertising and other profiling activities
- When you are asked to set the answers to authentication questions – especially if the service is of low value to you, there is no obligation to provide them with accurate answers
- Occasionally, use your favourite search engine to check for online information about yourself. You might be surprised what you find and you may be able to contact the website owners and have misleading or personal information removed
- If you can, encrypt your storage media. Hard disks, especially for laptops, and, if they carry sensitive information, removable media such as CDs or memory sticks
- Make sure you destroy media of which you are disposing and that contains personal information. Paper can be shredded, as can most optical media (although check your shredder). Hard disks are often resold and have regularly been found with sensitive personal data remaining (obviously, if you have encrypted the disc effectively, recovery is very unlikely)

Avoid storing information on online sites

Many vendors will ask if you wish to save your personal information so you can recall it later, if you wish to perform another transaction. The vendor may allow you to store your name, shipping and billing addresses, payment preferences and financial details, such as payment card numbers or bank account information. Having a vendor store this information poses multiple risks.

- You are increasing the number of places where your personal data exists and thereby increasing the number of opportunities for it to be compromised
- Vendors typically retain this data or an indefinite amount of time, thereby creating a higher probability that it can be compromised
- You are placing your trust in the vendor to protect this information. Even with sophisticated security, there is still a risk of the systems being compromised and the data stolen

Consider carefully whether the convenience of storing your personal information on a vendor's site outweighs the risk of having the information stored somewhere, which is out of your control. If you are making a one-time purchase, it is advisable not to store this information on the vendor's site.

Protect your PC

Some fraudsters use spyware or keylogger programs to steal personal information directly from your PC. These programs record all keystrokes, allowing identity thieves to learn the username and password you use to access your bank account or online merchant account. Others "sniff" unsecured wireless networks to gain access to shared folders on your PC.

Some simple steps can also help you protect your online shopping experience. These steps do not require any extraordinary effort, but can result in significant gains in the security of your personal computer. To thwart these efforts, be sure to:

- Install a personal firewall as well as anti-virus and anti-spyware software. Update virus and spyware protections regularly (daily if possible) and run full scans at least once a week
- Avoid downloading email attachments or clicking on a link in an email unless the message is from someone you trust
- Never provide sensitive information in an email. Remember that legitimate merchants, banks or brokerages will never ask for your username, password, PIN or other sensitive information in an email. Only fraudsters will
- If you're using a laptop, create a password to log in and access any information
- Always use a secure Wi-Fi (wireless) network. Set up a password to secure your home wireless network and avoid buying online or logging into bank and investment Web sites while on a public Wi-Fi network
- Disconnect from the Internet when you're not online
- You should always use a reasonably modern version of the operating system you prefer
- You must always keep your operating system up-to-date. Most modern operating systems will now provide some sort of automatic update system, which you should ensure is running correctly, and all the major vendors provide email or web-page notifications for security- significant patches
- Use a modern web-browser. There have been very significant security improvements in the recent generations of web-browsers so, regardless of which is your favourite, you should ensure that you are running the most recent production version and that you also keep this up to date
- Use browser security notifications. Some modern browsers, including the two market leaders (Microsoft Internet Explorer and Mozilla Firefox), will provide warnings if you are visiting sites that have been reported to them as possibly fraudulent. These have been shown[10] to help people recognise attempted frauds. If your favourite browser does not provide this functionality, there may also be appropriate independent vendor toolbars available[11]
- Run one reliable anti-virus product and keep it updated. Many computers come with limited-time free subscriptions to one of the major commercial products – you need to make sure that you purchase the on-going subscription or install an alternative product when this runs out. There are also a number of effective free-for-home-use products available. However, only install one product – if you have multiple versions running, they can interfere with each other, greatly slowing your computer down or possibly even allowing some malicious code to pass

10 Wu, Min et al., Do security toolbars actually prevent phishing attacks? Conference on Human Factors in Computing Systems, Montreal, 2006.
11 Your anti-virus vendor may provide a toolbar. Free versions are also available.

- Make sure your computer account requires a password to login. Not only does this protect your account if your computer is ever stolen, but it also provides additional security from malicious hackers who attempt to gain access to your computer
- Configure a screensaver and have it require a password to unlock the screen. This will prevent someone from gaining access to your computer while you step away. This is especially important if you use a laptop

Shopping safely

Even if you use the latest, most secure browsers and are using a PC equipped with a firewall, antivirus software and anti-spyware software, it is important to remain vigilant while online. Here are some ways you can keep yourself safe:

- Be wary of websites that are poorly built or programmed and don't provide any verifiable security information. If you are still not sure whether it is legitimate, email or call the company before providing it with any information
- Look for a padlock icon on any shopping site. To be meaningful, the padlock icon must appear in the actual browser interface – and not inside the content of the page itself
- Avoid sites that have obvious and abundant typographical errors
- Keep your computer software up to date
- Be careful what you do from an unprotected or unknown computer
- Be aware of the terms and conditions of the payments system you are using
- Watch out for postage and packing charges
- Remember, if you are comparing prices from outside of the European Economic Area, you may have to pay VAT and import duties.
- Use reliable merchants or managed marketplaces (such as Amazon or eBay) that have robust complaints procedures
- Avoid shopping from public computers. These are used by all types of people, including those who are not concerned or aware as you are of the need for security. These computers are often used, either intentionally or unintentionally to visit sites that contain malicious software. As a result, they can potentially contain malicious software, which will collect any information you type in, including usernames, passwords, and financial information, such as payment card numbers and banking information. Unless absolutely necessary, avoid using public computers for viewing or inputting sensitive information
- Remember the proverb, "If it looks too good to be true, it is too good to be true"

If you need help or further information contact your local European Consumer Centre[12].

Secure payment

There are a number of steps you can take to ensure the security of the payments you make online. These are:

- Use a low limit method of payment, where possible, such as a credit card with a low credit limit.
- Check your bank account or credit card statements after payment, and in any case regularly, for any suspicious transactions
- Use a temporary method of payment where possible
- Favour a credit or debit card issued by a bank that has fraud prevention services (check the bank website to find these details)

Know your rights

If anything goes wrong with an online purchase, it is essential that you know what rights you have to correct any errors or, otherwise, to be refunded. Remember that shopping online does not remove any of your fundamental rights and, often, will actually allow you additional ones. It is important that you realise what rights you may have in law, under the contract of purchase and under the terms and conditions of the payment method you have used.

12 European Consumer Centre Network (ECC-Net) http://www.ecc-net.info/

However, you do need to remember that, in many cases, the jurisdiction of the contract you have entered will be in the legal domain of the merchant or marketplace.

Purchasing online does not necessarily involve any reduction in the consumer rights you have and can even strengthen them.

- Goods must be as described– that is, the goods delivered must be of the appropriate functionality and quality, as described on the website and any options or variations you requested must be supplied. A merchant, for stocking or other reasons, may choose to send you a different product, but you do not have an obligation to accept this unless you have already indicated your agreement
- Goods must be fit for purpose – they must be intact when delivered; in date if they have a 'best before' or similar date and, if the goods break or are otherwise damaged in normal use, you are entitled to have this corrected if the goods are less than 6 months old
- You must receive the goods. If you haven't taken delivery of them within 30 days, you are entitled to a refund. Note that it will normally be the vendor, rather than you, who has the contract with the delivery company, therefore it is their responsibility to ensure delivery
- Under the EU Distance Selling Directive, you have the right to withdraw from the contract within 7 working days and return the goods. You can be required to pay for the return postage but, under a recent judgement, it has been confirmed that any original postage and packing charges should also be refunded. Different rules apply for some services and for goods that are perishable, or have been personalised
- You may have statutory or contractual rights for a refund from the provider of your method of payment. Statutory rules will be detailed in your local implementation of the EU Payment Services Directive.
- If you have bought through a marketplace site, the terms and conditions of that site may give you additional protection
- Regarding the payment for your goods, remember that under European law, once the payment is complete the seller must acknowledge receipt of your order. Therefore, you should receive a receipt for the payment processed

Some European governments provide specific protections for those who shop online. The UK's Data Protection Act, for instance, ensures that the information a business receives from you when you make an Internet purchase must be handled in the same way as information processed in a "bricks-and-mortar" shop. Merchants are not allowed to share your information with third parties without your consent.

If you suspect your identity has been stolen, contact your bank and request they flag your account and alert you to any unusual activity. Report the theft to major credit bureaus, and file a report with your local police department. You may also want to alert your passport office, in case someone tries to apply for a passport in your name. And be sure to document all conversations and communications, complete with names, numbers and dates.

Under European legislation for distance contracts/selling, you have the right to cancel the contract within seven days from the acknowledgement receipt of the order in the event of a duplicate payment. Regarding the delivery of the goods, they must be sent within 30 days. The legislation allows that in case of a dispute it is possible to take legal action in the national courts, or opt for an alternative dispute resolution.

Golden rules for shopping safely

When shopping online, you should consider the following golden rules:

Category	Recommendation	Description
Know your dealer	Check "terms and conditions"	Look closely at return and cancellation policy, delivery details and warranty information. Shipping fees, final costs and jurisdiction should be checked carefully. Consider making a personal copy.
	Check home country and address	There are Web shops, which look like a local dealer, but are situated in foreign countries. In the case of an international dealer, pay close attention to customs duty, tax and legal issues. As buyer you are responsible for such aspects as correct customs clearance.
	Be aware of fraud shops	Ensure you are visiting the Web shop you want to visit. There are fraud shops with very similar URLs to those of legitimate Web shops. Fraud URLs could be distributed via URL shorteners such as TinyURLs or within emails.
Protect your data	Use unique passwords	Don't use similar passwords at different shops. Use strong passwords.
	Check privacy policy	Which personal information of yours is stored for how long and for what purpose? When will your data be deleted? How is it protected?
	Only provide required personal information	Question all requested information within the Web shop - don't disclose any personal information that is not absolutely necessary for the online shopping process.
	Check for an encrypted connection (SSL) for personal data transfer	Secure Socket Layer (SSL) encrypts the communication between your browser and the web shop; see the section on SSL for further details.
	Payment process	Choose your payment method wisely. See section on Banks and Payment services for possibilities and risks in more detail.

Know your rights	Legal rights protect online customers	You should know applicable acts and regulations, such as the distance selling or warranty regulations. They may differ from state to state.
Know what you are buying	Check product details	Double check product price, amount, version, authenticity. Spelling mistakes in brand names should alert you – be aware of product piracy.
	Check delivered products	Are appearance, amount and workmanship as proposed? If there are any doubts, contact the dealer immediately in written form.
Be aware	Check bank account or credit card statements after payment	Check if the correct amount was withdrawn and if there are any unauthorised charges.

Showcase - book your holiday online safely!

Get Safe Online, the UK's national Internet security awareness initiative, has launched a campaign together with ABTA (the largest travel association in the UK) to highlight the risks of bogus online safety scams. The survey has showed that nearly 1 in 3 of web-users put themselves at risk when booking their holidays online. Over two-thirds of UK web users are unaware of most common tricks, such as holiday rental scams, unsolicited emails or phone calls from individuals or unknown organisations and almost 30% of web users book their holidays online without confirming the authenticity of the travel providers. To book your holidays more safely and be sure that you have made all the right steps, read the Get Safe Online travel tips available at www.getsafeonline.org.

Guidelines for online merchants

Selling goods and services online can provide retailers and manufacturers with many benefits, such as cost savings, extended customer base and more efficient sales processes. However, it is essential that, when creating an online e-commerce presence, organisations are aware of their responsibilities and obligations to their clients. The following is a number of steps that you should consider when developing your e-commerce presence.

Staff

- Since online merchants have to rely by definition upon Information and Communications Technology (ICT), you should adequately manage it. This means having a fully dimensioned and competent staff, which also includes significant security management expertise. This could be either sourced internally, or outsourced to companies specialising in this area
- You also need to train non-technical staff in their roles and responsibilities regarding the e-commerce site and ensure that they are aware of the rights of the customers and deal with them appropriately. Staff should also be trained in how to detect, report and deal with potential fraud

Secure your systems

- Ensure that the systems you install and which your e-commerce platform relies upon are secure. This means installing appropriate security systems to protect your website from attack by criminals, such as a firewall and Intrusion Detection Systems. Turn on all audit trails and log files and make sure that they are regularly and actively monitored. Audit trails not only provide you with an account of what events a visitor performed on your website, but can also assist you should you have to investigate a security incident. The log files on a system can also warn you about a potential attack, or can be used to deal with an on-going attack against your systems
- Use SSL certificates to secure the communication between your site and those of your customers. Make sure that you use SSL certificates provided by recognised and trusted vendors
- You should also regularly test your systems for security weaknesses, or vulnerabilities. These tests should help identify potential weaknesses that criminals could exploit. Should any vulnerabilities be identified, look at ways to address them
- When using online providers for your online shop, make sure to analyse the provider's contractual responsibilities regarding security

Website content

- Ensure that the content of your website is correct and that all pricing and other details are up to date and contain no errors. Having a lot of errors on your pages will not create confidence with customers who visit your site. You should also ensure that all pricing is correct and also includes shipping fees and taxes that may be applicable
- Make sure your privacy policy is readily available for visitors to your site to read and that you clearly state what your policy is regarding the collection and subsequent use of the data those visitors will provide
- Ensure that you have processes and procedures in place and staff trained to identify potential fraudulent activity. Should you detect fraud on your system, make sure you have the appropriate processes in place to deal with it

Regulatory and compliance issues

Ensure that you and your staff are aware of all the regulatory and compliance issues that your organisation and e-commerce site need to adhere to. In particular, you need to make sure that the following areas are addressed:

- Directive 97/7/EC, Protection of Consumers in Respect of Distance Contracts
- Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees
- The Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

You should also ensure that you are aware of any regulations specific to your local jurisdiction regarding banking, money transfers, money laundering and electronic commerce.

PCI DSS

Online merchants need to ensure that they do not become the weakest link for the security of their customer's cardholder data. They need to ensure that they boost customer confidence in their ability to take credit card payments online securely.

To do so they are advised to ensure that they themselves comply with PCI DSS. Most merchants are either at level 3 or 4 and, in order for them to validate their compliance, they need to do four things:

- Educate their employees on credit card security and generic security best practices
- Promote and implement strong security policies and procedures
- Scan their external IP addresses linked to payment systems quarterly using an Approved Scanning Vendor (ASV) fully approved by PCI SSC
- Complete a Self-Assessment Questionnaire (SAQ) and file it with their acquiring bank

This has to be a continuous process and the Self-Assessment Questionnaire must be filed each year. Employees are in scope if they have physical or logical (IT) access to credit cardholder data and they must be trained upon hire and at least once a year. There are many Approved Scanning Vendor providers for merchants to choose from and it is up to the merchants to ensure that they pass these scans every quarter. Self-Assessment Questionnaires can be downloaded free of charge form the PCI SSC site. However it is worth noting that a number of vendors offer fully integrated solutions for merchants to validate their compliance, using online tools. The advice to merchants is to ensure that the solution is comprehensive and does offer the four elements mentioned above – employee education, policies and procedures, scanning and Self-Assessment Questionnaires - as opposed to a subset of the overall compliance requirements.

Online merchants also need to familiarise themselves with the types of on-line fraud schemes on an on-going basis. They need to report fraud or suspected fraud attempts to the security departments of their payment service provider, or banks, as soon as they become aware of potential incidents.

This is why PCI DSS has made in-scope employee training mandatory, as part of requirement 12.6 of the standard. Raising security awareness of potential security issues and fraud is key to the fight against online shopping fraud. Merchants and consumers alike need to be aware, however, that the onus is on merchants to ensure that staff are pro-active and help fight the issue.

Merchants are also advised to review how they can combat online fraud using technology solutions to complement employee training and traditional security. If the merchant has a well-developed e-commerce online practice, they are advised to invest in financial crime and compliance solutions aimed at decreasing fraud losses, improving investigation efficiency and case management, increasing accuracy of detection, decreasing capital expenditure and support costs and reducing risk of sanctions and fines by regulators.

Conclusions

It is clear that online commerce in its many forms is here to stay. It will no doubt continue to grow and expand as the use of computers and technologies grow and expand. The use of new technologies will also provide many opportunities within this space.

Consumers can take advantage of the ease of use and benefits that online shopping can provide. Sellers can leverage the Internet to enable them reach customers that they otherwise would never reach and to provide new goods and services. Online shopping also can provide organisational benefits such as improved processes, better brand recognition, reduced costs and improved productivity.

However, just as the Internet provides both the consumer and the seller with many advantages, it also provides a number of risks that need to be recognised and managed. Criminals also recognise the benefits the Internet provides and they too will take whatever advantages they can to steal, defraud and commit crimes.

Consumers should ensure they follow the Golden Rules for Shopping Safely and merchants looking to sell products and/or services online should follow the Guidelines for Online Merchants, both of which are outlined in this report.

With proper awareness and education, both the consumer and the vendor can be more confident in their ability to conduct business online safely and securely.

References and sources for further reading

Aboutidentitytheft.co.uk, *Your Consumer Rights Online*, available at http://www.aboutidentitytheft.co.uk/consumers-rights-online.html (last visited April 14, 2010)

Atif Mushaq, *Man in the Browser: Inside the Zeus Trojan*, Threatpost, 19th February 2010 http://threatpost.com/en_us/blogs/man-browser-inside-zeus-trojan-021910

Christopher Weber, et.al. *Life Cycle Comparison of Traditional Retail and E-commerce Logistics for Electronic Products: A Case Study of buy.com*, Green Design Institute, Carnegie Mellon University, December 8, 2009.

Donna L Montaldo, *Is Shopping Online Really Cheaper?* http://couponing.about.com/od/bargainshop/a/onlinecheaper.htm (last visited November 2010)

Dushyant Pota, *Understanding online retail: A classification of online retailers*, The Journal of Computer Information Systems, Saturday, January 1 2000, last viewed at http://www.allbusiness.com/marketing/strategic-marketing/1069372-1.html on April 20, 2010.

ENISA Report, *Online As Soon As It Happens*, February 2010 http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens

European Commission, *The proposal for a directive on consumer rights: impact on level of national consumer protection – Comparative table,* http://ec.europa.eu/consumers/rights/docs/comparative_table_en.pdf

European Commission, *Proposal for a Directive on consumer rights*, http://ec.europa.eu/consumers/rights/cons_acquis_en.htm#top

European Commission, *On the Implementation of the Distance Selling Directive*, http://ec.europa.eu/consumers/cons_int/safe_shop/dist_sell/index_en.htm

European Commission, *eYouGuide to your rights online*, http://ec.europa.eu/information_society/eyouguide/index_en.htm

EU Data Protection Directive 95/46/EC http://eur-lex.europa.eu/Notice.do?val=307229:cs&lang=en&list=307229:cs,&pos=1&page=1&nbl=1&pgs=10&hwords=95/46/EC~&checktexte=checkbox&visu=#texte

EU Electronic Commerce Directive http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF

EU Electronic Privacy Directive http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

EUROSTAT's *Internet usage in 2009 - Households and Individuals survey* http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-09-046/EN/KS-QA-09-046-EN.PDF

Forrester Group, *US Online Retail Forecast, 2009 to 2014* http://www.forrester.com/rb/Research/us_online_retail_forecast%2C_2009_to_2014/q/id/56551/t/2

Forrester Group Forecast, *Double-Digit Growth For Online Retail In The US And Western Europe* http://www.forrester.com/ER/Press/Release/0,1769,1330,00.html

Friberg, Richard & Ganslandt, Mattias & Sandström, Mikael, 2001, *Pricing Strategies in E-Commerce: Bricks vs. Clicks*" Working Paper Series 559, Research Institute of Industrial Economics.

Jones, Andrew et al., *The 2007 Analysis of Information Remaining on Disks offered for sale on the second hand market*., Int. J. Liability and Scientific Enquiry. 2009.

Juliet Sneddon, *Online Shopping*, http://wiki.media-culture.org.au/index.php/Online_Retail last viewed April 20, 2010

Michael Rappa, *Business Models on the Web*, http://digitalenterprise.org/models/models.html last viewed April 20, 2010

OWASP, *Overview of the Man in the Middle Attack*, http://www.owasp.org/index.php/Man-in-the-middle_attack last viewed August, 2010

PCI Security Standards Council Site
https://www.pcisecuritystandards.org/

PCI Security Council Approved Companies and Providers –
https://www.pcisecuritystandards.org/qsa_asv/index.shtml

Rand, Dennis, *Social Networking Risk – Who Do You Want to be Today?*, CSIS Security Group, May 07

Rand, Dennis, *Threats when using Online Social Networks - 5 month later* CSIS Security Group, Oct 07.

Retail Research (CRR) *eCommerce and Online Retailing Report*
http://www.retailresearch.org/onlineretailing.php

Shari Waters, *Selling Online - Retailing Storefront Alternatives*,
http://retail.about.com/od/location/p/online-sales.htm

The Microsoft Internet Explorer browser version 8.0
http://www.microsoft.com/security/products/ie8.aspx

The Mozilla Firefox browser version 3.0
http://www.mozilla.com/en-US/firefox/features/

The Register, *Cosmic 419er Lost In Space* - http://www.theregister.co.uk/2004/04/16/cosmic_419er/, Apr 04.

VeriSign, *Fraudsters Shift from Financial Targets to Stealing Personal Information, VeriSign's Online Fraud Barometer Research Reveals*, Press Release, March 17, 2010, available at http://www.verisign.co.uk/press/page_20100317.html (last visited April 14, 2010)

VeriSign, *VeriSign Internet Trust Index*, March 2010, available at https://www.trustthecheck.com/assets/VeriSign_Internet_Trust_Index_March_2010.pdf (last visited April 14, 2010)

VeriSign, *Research Reveals 88% of UK Web Users Unable to Spot Phishing Sites*, Press Release, June 11, 2009, available at http://www.verisign.co.uk/press/page_061109.html (last visited April 15, 2010)

VeriSign, *Internet Trust Index Pinpoints Who Trusts the Internet, Who Doesn't, and Why* http://www.trustthecheck.com/trustindex/default.aspx, March 2010

VeriSign, *Fraudsters Shift from Financial Targets to Stealing Personal Information, VeriSign's Online Fraud Barometer Research Reveals* http://www.verisign.co.uk/press/page_20100317.html, March 2010

Wu, Min et al., *Do security toolbars actually prevent phishing attacks?*, Conference on Human Factors in Computing Systems, Montreal, 2006.

Catalogue number: TP-31-10-734-EN-C
ISBN-13: 978-92-9204-050-5
DOI: 10.2824/19287

TP-31-10-734-EN-C

enisa
European Network and Information Security Agency

ISBN-13: 978-92-9204-050-5

PO Box 1309, 71001 Heraklion, Greece Tel: +30 2810 391 280
www.enisa.europa.eu