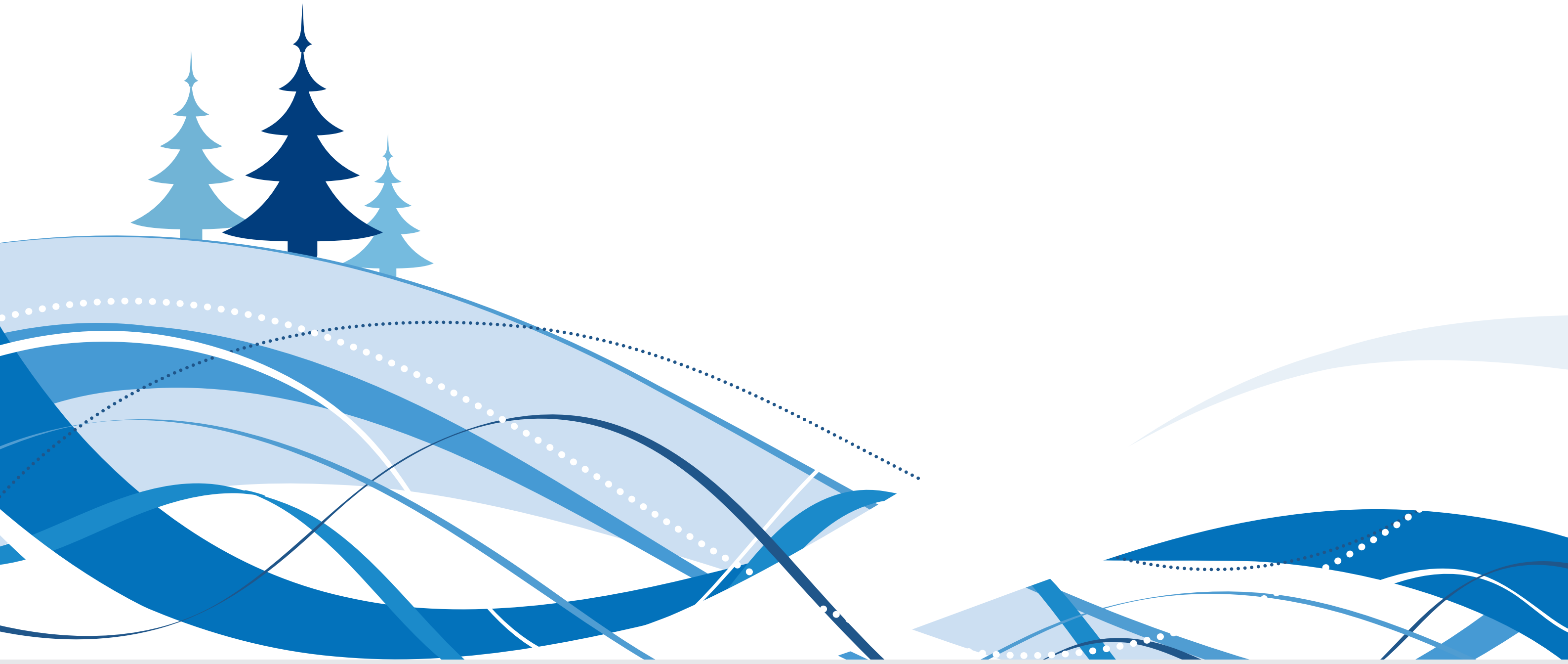
Practical tips for a **Safe Christmas**

PANDA
SECURITY

CONTENTS



The Christmas holidays normally see an increase in the activity of cyber-crooks. The reasons are simple: with more spare time on their hands, more people connect to the Internet. Consequently, the possibility of people falling victim to online crime is statistically higher.

Here we will take a look at the main risks to watch out for over the holiday period, and how to prevent them.

1. ONLINE SHOPPING

With many people now shopping on the Web, **the number of online transactions increases over Christmas**. For example, the Monday immediately after Thanksgiving this year –a day known as Cyber Monday since it has become the start of the online Christmas shopping season- the number of Americans who made an online purchase increased by 38 percent with respect to 2006[1].

Last year, **13.5 million2 Americans** did their Christmas shopping online.

Cyber-crooks are obviously aware of this increase in online trade over Christmas and therefore step up their attacks. Consumers can be attacked on several fronts. One of the main strategies is **phishing**, which consists of spoof emails that purport to come from an online bank or shop. Users are asked to click on a link and enter their bank details. If they do, any data they enter could end up in the hands of cyber-crooks.

Last year, the number of phishing attacks launched in December rose to **23,000**[3], 56% more than the previous year.

Trojans are another risk that consumers face. Banker Trojans, in particular, are designed to steal users' bank details (passwords, account numbers…).They count 18,59% out of total samples of malware created in 2007[4]. They can capture keystrokes and even redirect users to spoof banking sites. It is vital therefore, that online consumers make sure their computers are malware-free before carrying out online transactions.

1- http://www.cnnexpansion.com/economia/2007/11/28/eu-logra-record-de-compras-on-line
2- http://www.bnd.com/business/story/193659.html.
3- Data from the Anti-Phishing working Group.
4- Data from PandaLabs, the malware analysis and detection laboratory at Panda Security.

How do Trojans reach PCs? Trojans do not spread on their own, they require user collaboration. They 'disguise' themselves as files or links that contain photos, movie trailers and so on, to entice users into opening them or clicking them. If users open the file or click on the link, they could actually be dropping a Trojan onto the system.

Online consumers should take great care, since according to 2006 estimates, each victim lost on average €6,383[5] through these techniques.

Spoof auction pages or online stores are also a serious risk for online buyers. Many fake sites offer products at unbelievable prices, so unbelievable in fact, that users should think twice before believing them. Users who purchase items on those sites, probably won't receive the product and are unlikely to see their money again. It is always a good idea to check out the reliability of the page before purchasing anything.

An easy way of checking a website's reliability is to make sure the connection is made through the SSL protocol. This protocol allows the data between the PC and the server to be transferred securely and privately, so the information doesn't end up in the hands of third-parties. Another simple way is to type the name of the page in a search engine and read other consumers' opinions. If there are numerous complaints about defective products, or products that do not reach the recipient, you should think again before purchasing an item from that website.

5- Data from the Anti-Phishing working Group.

2. ONLINE GAMES

Búsqueda en Google: virus - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Multimedia
Dirección http://www.google.com.ar/search?hl=es&q=virus&meta=
msn Buscar Resaltar Opciones Ventanas emergentes bloqueadas (6) Hotmail Ir Vínculos
Top Sellers in Sports & Outdoors
VIEW CART | WISH LIST | YOUR ACCOUNT | HELP
WELCOME YOUR STORE BOOKS APPAREL & ACCESSORIES ELECTRONICS TOYS & GAMES KITCHEN & HOUSEWARES COMPUTER & VIDEO GAMES SEE MORE STORES
GIFT CERTIFICATES | INTERNATIONAL | NEW RELEASES | TOP SELLERS | TODAY'S DEALS | SELL YOUR STUFF
Sign in using our secure server

Change your e-mail address and sign in

Enter your old e-mail address:
(Use the old address associated with your Amazon.com account.)

Enter your password: ********
Forgot your password?

Enter new e-mail address:
(We'll send a message to your new e-mail address confirming the change.)

The secure server will encrypt your information. If you received an error message when you tried to use our secure server, sign in using our standard server.

Where's My Stuff?
- Track your recent orders.
- View or change your orders in Your Account.
- See our animated demo!

Shipping & Returns
- See our shipping rates & policies.
- Return an item (here's our Returns Policy).

Need Help?
- New customer? Click here to learn about searching, browsing, and shopping at Amazon.com.
- Forgot your password? Click here.
- Redeem or buy a gift certificate.
- Visit our Help department.

At Christmas most people have more spare time on their hands, much of which is spent playing online games with other remote users. In the last few months, numerous malware variants designed to steal online game credentials have been detected.

Cyber-crooks steal credentials to sell them on the Internet black market, where they can fetch incredibly high prices. The reason is that many objects, functions, etc. in these online games are accumulated through the skill and experience of players. There are many who are unable to reach this level and are prepared to pay significant sums to obtain these virtual assets. Cyber-crooks take advantage of this to sell them to the highest bidder on forums, auction pages, etc.

Another problem with online games is that many of them allow users to create profiles. The profiles often include players' email addresses so they can share tricks and experiences. Cyber-crooks use this information to customize emails claiming to contain game or image plugins to entice users into opening attached files or click on a link. If they do, they may actually introduce malware onto their system.

The sending of files claiming to contain the game itself or the distribution of these files through P2P networks, etc. are other methods used by cyber-crooks to exploit users' interest in these games and distribute their creations.

3. INSTANT MESSAGING AND MAIL

The use of **instant messaging** as a means of communication is increasingly widespread. Tools such as MSN Messenger, Yahoo!Messenger, etc. are some of the most widely-used, especially by young people. They have consequently become one of cyber-crooks' favorite channels for distributing their creations.

They usually send links or files that appear to come from a known contact, but it is really a worm that attempts to spread to other users. If users click the link or download the file, they will be infected.

A similar technique is used to distribute malware through **email**. One of the most commonly-used methods at this time of year are free Christmas cards, which offer users fun greeting cards to send their family and friends. To obtain them, users are told to click a link or download a file. Either way, users are infected with malware.

On other occasions, malicious codes **take the form of movie trailers or codecs**, taking advantage of the numerous movies released during Christmas. Once again, it is bait to entice users into carrying out an action that will lead to infection.

4. PRACTICAL TIPS FOR A SAFE DIGITAL CHRISTMAS

1. Make sure there are no active viruses on your PC before you shop or bank online. To do this, add proactive technologies to your traditional antivirus. These technologies can detect threats without requiring updates and use "**second opinion**" antivirus tools to make sure your PC is malware-free.

2. **Take no notice of spam (advertising) messages** or those that claim to come from financial entities and request confidential data

3. **Check out** the seller's reputation before shopping online.

4. **Keep the operating system and the applications on your system up-to-date**. System vulnerabilities can be an entry point for malware, and can allow cyber-crooks to take control of your PC.

5. **Do not run files or click on links from suspicious sources**. Additionally, if you receive a file through instant messaging, make sure it is sent by one of your contacts and that it is not malware.

6. Never pay for anything online unless you can completely **trust the seller**. If you are bidding for an item in an online auction, do not trust the offers you receive, unless they come from the auctions' own portal. You could end up empty-handed, with no product or money.

7. **Do not send confidential data via email**, instant messaging, chats or similar channels.

IN SHORT

As Christmas provides cyber-crooks with an ideal environment, due to the increase of online transactions and users' spare time, it is one of the most dangerous seasons for Internet users. Unless users want their money to end up in cyber-crooks' hands, they should stay on the alert and take adequate security measures.

PANDA
SECURITY