

# On the 12th day of Christmas a cyber criminal gave to me...a Facebook profile worth 89p

Submitted by: Onechocolate Communications

Tuesday, 16 December 2008

---

Find out how much your personal and financial information is worth to the Cyber Mafia. Are your details on their 2008 shopping hit list?

The run up to Christmas is a peak time for online crime. Research from Trend Micro, one of the world's leading internet security companies, revealed that cyber attacks rose 500% in the key shopping period between September and December in 2007. And we're already seeing a similar trend in 2008.

But did you know that cyber criminals are making a serious profit of selling our stolen personal and financial details on the "online black market" this Christmas? Whilst you're writing your shopping list, the online mafia is drawing up their very own list of most wanted gifts.

This is what the 12 days of Christmas looks like to an online thief:

- Day 1: Advanced malware package worth £1400
- Day 2: 10,000 jeopardised PC's with dangerous spying software installed worth £700
- Day 3: Basic malware pack, simple box of tricks for criminals to obtain your info for £700
- Day 4: Guaranteed undetected Trojan, used to steal information for £60
- Day 5: Your stolen bank details starting at £35
- Day 6: Stolen credit card details starting at £25
- Day 7: 30,000 UK based email addresses for spamming purposes for £5
- Day 8: 1,000,000 international email address for spamming purposes just £4
- Day 9: Login for MySpace account just £1
- Day 10: Login for Skype account a bargain at £1
- Day 11: Online computer game account £1 only
- Day 12: Facebook profile just 89p, 10p more than a single on iTunes!

"We still give away a huge amount of personal information on social networking sites like Facebook and MySpace. Hoards of cyber criminals are also drawn to these sites as crucial data, needed for identity theft, tends to be readily available - including email addresses, names and birthdays for example", says Rik Ferguson, Trend Micro.

"Whether you're going online to use Facebook, doing your banking or Christmas shopping you should be aware that hacking activity and identity theft tend to increase during certain times of the year. As we approach Christmas we urge users to apply a certain sense of caution when it comes to the sites they visit and giving away personal information."

Here are Rik's top tips for staying safe:

1. Look for the padlock

If you can see it in the bottom right hand corner of your browser it's a good sign that the site you

are on is secure.

## 2. Vary your passwords

It might be a pain to have to remember more than a couple of different passwords, but otherwise if someone finds out one, they've found the lot. You should definitely use a different one for online banking, and change it every few months.

## 3. Use the privacy settings on social networking sites

And report any suspicious behaviour to the group moderators.

## 4. Clean your machine for free!

It's the only way to make sure that there is nothing nasty lurking on your computer watching what you do. If you're worried you can scan and clean your machine for free by visiting [www.trendmicro.com/housecall](http://www.trendmicro.com/housecall).

## 5. Always use protection software

To ensure you are protected at all times invest in some software to help you stay safe online. Visit [www.trendmicro.co.uk](http://www.trendmicro.co.uk) to find out more.

For more information please contact Sophie Brown, Clare Hamilton-Eddy or Matt Churchill at Chocolate Communications on 020 8322 1922 or email [trendmicro@chocolatecom.co.uk](mailto:trendmicro@chocolatecom.co.uk).