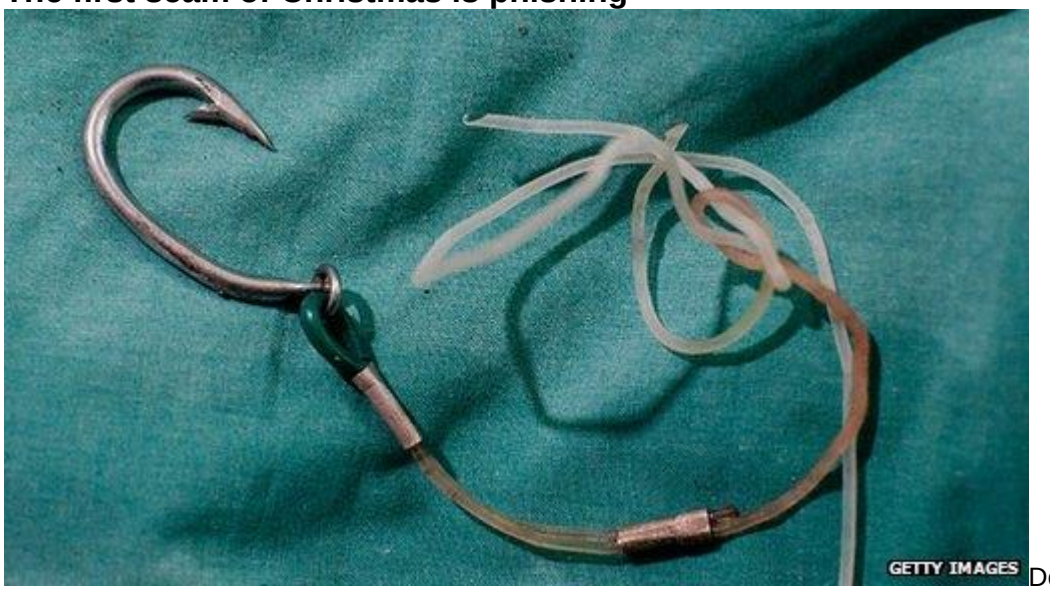
The 12 cyber-scams of Christmas

By Prof Alan Woodward Department of Computing, University of Surrey

This Christmas looks like being a bumper one for online shopping but not everyone is filled with the festive spirit and some have already set online traps they hope you will fall into.

Here are twelve cyber-scams to watch out for this Christmas:

The first scam of Christmas is phishing



Don't get hooked by fake messages

They've been around for years and we've all received a version.

Fraudsters send you a message and attempt to make you click on a link to a fake site or open some malware that infects your machine.

They may be old but they have evolved and some are very cleverly targeted (known as spear phishing). Imagine you are placing orders on a well-known website for gifts. Suddenly you receive an email - apparently from that very site - saying that there is a problem with your last order and can you please "click here" to attend to the problem.

Logos, email addresses, even the link might look genuine but you'll get more than you bargained for if you do as the email asks. Check twice and click once.

The second scam of Christmas is the fake virus checker

Beware of alerts promising to knock out malware that doesn't really exist

You search for that elusive gift, and finally you're led to a site that appears to sell just what your nearest and dearest want.

But wait, a message flashes up saying that your machine is infected… but don't worry just download the free virus check shown and your problem will be solved.

By downloading it you will actually be infecting your machine and your problems will only just have begun. Install a good virus checker before you go online.

The third scam of Christmas is the fake upgrade

Promised upgrades don't always deliver

As the Christmas spirit gets going we all send each other links to jokes and videos, on Facebook, by email and via Twitter.

Now imagine you arrive at one of these sites and it tells you that you don't have the latest Flash Player so you can't watch that funny video, but not to worry click here and you can get your upgraded player immediately.

Not only will this "upgrade" be malware but that malware will go on to send messages to all your friends telling them to go see the "funny" video.

The fourth scam of Christmas is the "current news scam"

Fraudsters are more than willing to take advantage of the news

People will use major world events to scam you out of money, regardless of how sad the event may have been. We saw it with Typhoon Haiyan in the Philippines.

Difficult to believe in a season of goodwill but before the aid agencies had reached the poor people affected there were already scam emails and associated websites asking you to donate.

They look genuine but don't be fooled. The money goes nowhere but to the scammers.

The fifth scam of Christmas is the illegal "cracked" download

Beware offers of "cracked" products offered on the net

Many will be buying laptops or other computing devices for under the tree.

They are expensive and there are many tempting offers to buy incredibly cheap operating systems, office products or other tasty goodies. There are even more tempting opportunities to download "free" copies of "cracked" pirated software.

However, not only are you likely to find that the download is an illegal copy - and may not actually run or has an invalid key - but also that it comes with a hidden present: malware.

Buy from reputable sites and remember if it's too good to be true then it probably is.

The sixth scam of Christmas is the drive-by download

When speeding through sites take care with links that take you to unexpected places

Sadly you do not have to agree to download software from a malicious site for it to happen. There are ways in which malware can be wheedled on to your machine just by visiting a site.

We all roam randomly around the internet, especially when looking for presents, so it is hard to avoid such sites. However, try to watch for a trail that leads you into totally uncharted waters. It's difficult, but think before you click.

And, keep your virus checker and your browser up to date. Both increasingly afford some protection again this type of scam.

The seventh scam of Christmas is the fake free wi-fi

Be suspicious of wi-fi connections labelled "free" if you do not know who is providing them

For those who do venture out you will doubtless take refuge at some point in somewhere like a coffee shop, and often it appears to have free wi-fi.

Such wi-fi connections should be considered insecure, so you should not visit any site where you need to enter credentials, card details or the like.

All of that might be visible to others who can monitor your insecure connection to the free wi-fi.

The eighth scam of Christmas is the wi-fi probe

Are you aware of all the information your mobile is sending?

Something few realise is that when we connect our mobile phone to a wi-fi, it keeps a record of the connection.

Thereafter if the device is not connected to a hotspot, it continues to send out requests to connect to all the previous networks to which it had linked.

These can be read and we are revealing all wi-fis we have previously joined.

In effect, your movements can be tracked and often your home network will even reveal where you live just by the name you have given it.

Don't give scammers information they might use against you in some form of con.

The ninth scam of Christmas is a combination of the last two

Leaving your wi-fi switched on all the time can leave you exposed

If you keep your mobile wi-fi turned on there are methods whereby, as your mobile sends out a request to connect to a hotspot, a scammer can then pretend to be that very wi-fi.

Your mobile is relieved to have found a connection it knows and so attempts to create a link, potentially giving away your wi-fi password.

Worse still, your mobile might think it has a secure connection and start to send other data that can be picked up by the scammer.

This and the two previous scams can all be stopped by simply turning off your wi-fi on your mobile's settings when not on a hotspot you trust.

The 10th scam of Christmas is the insecure website

Look out for a padlock in your browser to check you have a secure connection

Whether intentional or not, some websites still ask you for your credit card details - and much other valuable personal data - without offering a secure connection.

Know how your browser tells you that you have a secure connection - look for the padlock symbol or change of coloured address bar or whatever it is.

If you don't have a secure connection don't trust that site with your details.

They either can't be bothered, in which case they don't deserve your custom, or they're a fake.

Even if it is a secure connection make sure you click on the padlock symbol or similar to check that the site is registered to who you think it is.

The 11th scam of Christmas is the Man In The Middle (MiTM)

A Man in the Middle add-on may be watching over everything you are doing

There is no point in having a secure connection to your bank or shopping site if there is a piece of software sitting on your machine that can read all of the data before it is secured for transmission.

A particularly common MiTM scam is for a "helper" application that has been installed to make your life easier when using your browser.

This helper may be helping itself to anything you enter on the screen.

The safest way to avoid this is to ensure that you have no "add-ins" running.

If you know how, you can try this by manually configuring your browser but there are tools available, often from the banks free of charge, to do this for you.

The 12th scam of Christmas is the nastiest of them all: the phone call

It is worth being sceptical about whether the person calling you is who they say they are

You're having trouble with that new laptop you bought as a present. You've just about got it running but you can't quite figure out how to finish it off.

All of the sudden the phone rings and a voice says: "This Microsoft/Apple/Google/Dell/HP we see that you have managed to connect to the internet using one of our machines/software but look like you could do with some support. We're here to help you. All we need is your username and password…"

These scammers work on the principle that eventually they will find someone in exactly that position and upon receiving such a call the frustrated user is very likely not to question but rather welcome the caller.

All this caller is trying to do is help themselves to your login details and steal valuable data from your machine.

Sadly, there are more than 12 scams to watch out for, but be particularly aware of those scams that take advantage of the time of year.

Context is everything to the successful scam. If it appears relevant, useful or personal it is much more likely to succeed.

Prof Alan Woodward lectures at the University of Surrey's department of computing and is chief technology officer at the consultancy Charteris