BBC NEWS
TECHNOLOGY

17 December 2012 by Prof Alan Woodward
Department of Computing, University of Surrey

Viewpoint: How hackers exploit 'the seven deadly sins'

The phenomenon of "social engineering" is behind the vast majority of successful hacking.

This isn't the hi-tech wizardry of Hollywood but is a good, old-fashioned confidence trick. It's been updated for the modern age, and although modern terms such as "phishing" and "smishing" are used to describe the specific tricks used, they all rely upon a set of human characteristics which, with due respect to Hieronymus Bosch, you might picture as the "seven deadly sins" of social engineering.

Apathy:
To fall for a confidence trick, or worse, we assume others "must" have taken the necessary steps to keep us secure. Sadly this leads to a lack of awareness, and in the world of the hacker that is fatal. When we stay in a hotel and we programme our random number into the room safe to keep our belongings secure, how many of us check to see if the manufacturers override code has been left in the safe?It's nearly always 0000 or 1234 so try it next time.

Curiosity:
Humans are curious by nature. However, naive and uninformed curiosity has caused many casualties. Criminals know we're curious and they will try to lure us in. If we see an unfamiliar door appear in a building we frequent, we all wonder where it leads. We might be tempted to open it and find out, but in the online world that might just be a trap waiting for an innocent user to spring it. A colleague built a website that contained a button that said Do Not Press, and was astonished to find that the majority of people actually pressed it. Be curious, but exercise a healthy degree of suspicion.

Gullibility:
It is often thought of as a derogatory term, but we all suffer from this sin. We make assumptions. We take others at face value, especially outside of our areas of expertise. Put a uniform on someone and we assume they have authority. Give an email an official appearance by using the correct logo and apparently coming from the correct email address, and we might just assume its real, regardless of how silly its instructions might be. All of this can be easily forged online, so make no assumptions.

Courtesy:
We quite rightly all teach our children to be polite. However, politeness does not mean you should not discriminate. If you do not know something, or you feel something doesn't feel quite right, ask. This principle is truer than ever in the online world, where we are asked to interact with people and systems in ways with which we are quite unfamiliar. If someone phones you out of the blue and says they are

from your bank do you believe them? No. Phone them back. And by the way, use a mobile phone as landlines can remain connected to the person who made the call in the first place and so while you might think you're phoning the bank on a valid number you're just talking to the person who called you.

Greed:
Despite what we'd like to think we are all susceptible to greed even though it might not feel like greed. Since its inception, the very culture of the web has been to share items for free. Initially this was academic research, but as the internet was commercialised in the mid-1990s, we were left with the impression that we could still find something for nothing.

Nothing is ever truly free online. You have to remember that if you're not the paying customer, you're very likely to be the product. In the worst case, you might find that you have taken something onto your machine that is far from what you bargained for.

Many pieces of malware are actively downloaded by owners unaware that the "free" product contains a nasty payload, even if it also appears to do what you expected of it.

Diffidence:
People are reluctant to ask strangers for ID, and in the online world it is more important than ever to establish the credentials of those whom you entrust with your sensitive information. Do not let circumstances lead you to make assumptions about ID. For example, if someone from "IT support" calls you and asks for your password so they can help fix your problem, how do you know they haven't called everyone else in the building first until they found you who have really got a problem? This is a well-known attack. If someone has a problem with proving who they are, you should immediately be suspicious.

Thoughtlessness:
Thinking before you act is possibly the most effective means of protecting yourself online. It is all too easy to click that link. Stop. How many of us when reading an apparently valid link in an email would bother to check whether the link is actually valid or whether instead it takes you to a malicious site.

It's horribly easy to make links look valid so try hovering your cursor over the link for a few seconds before clicking to see what the real link is: the true link pops up if you give it a moment. As cynical as it may sound, the only answer is to practice your A-B-C: Assume nothing, Believe no-one, and Check everything

With more Christmas shopping expected to be done online this year than ever before, you should watch out for those that would exploit the deadly sins.
Don't give criminals the chance to ruin your holiday season, and remember that a little bit of paranoia goes a long way online.

Alan Woodward is a visiting professor at the University of Surrey's department of computing. He has worked for the UK government and consults on issues including cybersecurity, covert communications and forensic computing.