INTERNET NEWS

# How social engineering works

## In Depth: Think like a social engineer and you won't get caught out

*By Jon Thompson*

Saturday at 12:00 GMT | Tell us what you think [ 0 comments ]


There's plenty of valuable social engineering information to arm yourself with at www.social-engineer.org

Social engineering means different things to different people.

If you're a conman on a street corner, social engineering is a way to get money out of unsuspecting punters and steal goods.

If you're in a pub, it's a way to ensure that you're served first. If you're a magician, it can form the basis of an act. If you're a salesman, it's a way to get more sales.

But if you're a hacker, social engineering is far more: it enables you to get whatever you want from people. You can have them give you passwords, credit card details, and even access to secure places.

Many other cyber-attacks require an element of social engineering, and the techniques used are as advanced as other areas of online crime. At their heart is the basic human tendency to trust authority, and that trust sometimes comes at a very high price, as increasing numbers of people are discovering.

**Microsoft calling**

There's a new social engineering attack doing the rounds, which is designed to get you to give away all the details required to use your credit card online. Interestingly, it doesn't exploit your use of your computer at all, merely pretending that there's a problem with it.

The attack begins with an unexpected phone call, and it's a great way to learn about just how devious social engineering attacks can be and arm yourself against it and similar approaches.

All successful social engineering hacks begin with a process called pretexting. This creates a believable reason for the attacker making initial contact. Fear and greed are major human motivating factors, so the pretext is usually designed carefully to set the scene by giving the person being attacked the feeling that they've either inadvertently done something terribly wrong, or that they're in danger on missing out on something of value.

The new scam begins with a call supposedly from your ISP or even Microsoft itself. It seems obvious in the cold light of day that Microsoft isn't about to begin calling individual home users, and won't necessarily know who those users are, but a carefully crafted pretext for the call can make everything seem to be innocent and entirely reasonable.

Simply calling a random number from the phone book and insisting you're from Microsoft isn't enough to make the scam work, however. The call needs to be set in a believable context. This is achieved by playing a recording of a busy office in the background while the call is being made. The victim naturally assumes that the background noise is real, perhaps from a large call centre, which lends the situation an air of authenticity.

The caller must also appear to be in authority. The caller explains that Microsoft has had complaints that the victim's computer has been sending out spam, or perhaps worse. He might even give some examples and ask the victim to state truthfully if he or she has any knowledge of what's going on. The fear that a statement like this can generate in the minds of those not well

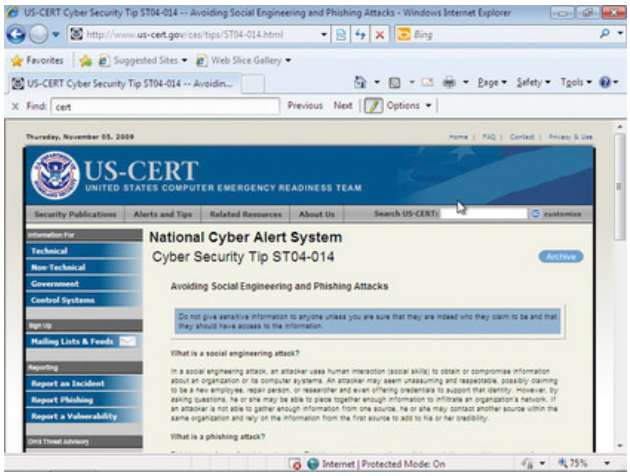
versed in online security can be enough to gain their complete compliance with whatever instructions follow.

**Fear factor**

After ramping up the fear of inadvertently doing something wrong, the attacker phrases his instructions to sound like an easy way out of the situation. He says that it doesn't matter because he can fix the problem almost immediately.

With the victim's permission, he can access the troublesome computer and remove the supposed malware, further explaining that to keep things legal, he needed to call to gain the victim's permission. In a situation like this, the naïve computer user is highly likely to accept this apparently easy and official way out of a sticky situation. To the attacker, however, this sign of compliance indicates that the victim is under his influence.

To further cement the belief in the authenticity of the call, and to deepen the control he exercises, the attacker may ask the victim to open a command line, display the machine's IP address using the ipconfig command, and to call it out to confirm that the right computer is to be accessed before proceeding. The fact that this IP address is local to the victim's ISP and cannot be seen by the wider internet further proves to the attacker that the victim is both clueless and compliant.




There are then a couple of minutes of apparent typing as the attacker claims to be accessing the victim's PC, possibly uploading anti-malware software, cleaning the system, and confirming that everything is in order. The attacker then gets to the real purpose of his call: the fee.

He explains that the victim will, unfortunately, have to bear the cost for the service he's just provided. After all, it was the user who let his PC get into such a terrible state. It'll be nothing expensive, just a few pounds for the engineer's time. However, he explains, the victim can make a saving on this bill by paying now, over the phone. All he needs is a credit card. You can guess the rest.

The victim believes his computer has been fixed and that Microsoft is wonderful for doing so – right up until he receives his next credit card statement. The assumption of trust in the person asking for information, established through careful attention to detail on the part of the attacker, allied to ignorance of the realities of online life, make this a social engineering attack that we're sure to see far more of over the coming years.

Indeed, one of the hallmarks of the information age is the way in which malicious activity evolves and develops over time. Old hacks never die, they simply evolve, and social engineering is no exception.

**Call for help**

Some social engineering attacks don't have to be so well planned, just carefully targeted. In Japan, one particularly successful form of attack is becoming big business by cynically targeting elderly victims with a blunt demand.

It begins when the victim receives a frantic phone call. "It's me! I'm in trouble and I need you to transfer some money quickly," is the type of call no parent or grandparent ever wants to receive. For an elderly relative, it can be horrifying.

As with the Microsoft phone attack, the attacker offers an immediate way out of the problem. Transfer several thousand Yen to a wire transfer service or bank account and everything will be fine.

Despite its bold simplicity, the 'Hey, it's me!' attack gains in popularity every year. According to Symantec, the Japanese National Police Agency recorded 20,000 cases in 2008 – up from 17,930 in 2007. In some areas, police

**How to create your own free computer forensics kit on a USB drive**

Criminals beware

**Tools and tricks of the white hat hackers**

How the security pros find and fix dangerous exploits



**GET MORE FROM TECHRADAR**

- Hands on: Google Nexus S review
- 20 best mobile phones in the world today
- Motorola Defy
- HTC Desire Z
- Microsoft Kinect for Xbox 360
- HTC Desire HD
- LG Optimus 7
- HTC HD7
- HTC 7 Mozart
- Samsung Omnia 7
- Amazon Kindle 3
- Best netbook revealed: the top 15 in the world today
- BlackBerry Torch
- Samsung Wave
- Best TV 2010: top-rated TVs revealed
- Samsung Galaxy S
- HTC Wildfire



**LATEST JOBS FROM TECHRADAR**

Search all IT jobs

**Support Analyst - 6 month contract**
£150 - £185 per day • United Kingdom - England - London - City

**Financial Application Developer - Agresso**
£400 per day • United Kingdom - England - London - City

**Jr .NET, SQL Developers,recent grads w elcome -excellent careers**
£22000 - £27000 per annum + + bonus, benefits, good career! • United Kingdom - England - London

**Senior Customer Service Support Administrator**
£21000 - £26000 per annum • United Kingdom - England - South East

**Netw ork Support Analyst - CISCO**
£250 - £300 per day • United Kingdom - England - South East

**Analyst Web Developer ASP.NET/ SQL / VB.NET- Yorkshire**
£26000 - £27999 per annum + £25000-£28000 +Pension +Company Benefits • United Kingdom - England - Yorkshire

officers have even been assigned to ATMs to warn people about the problem.

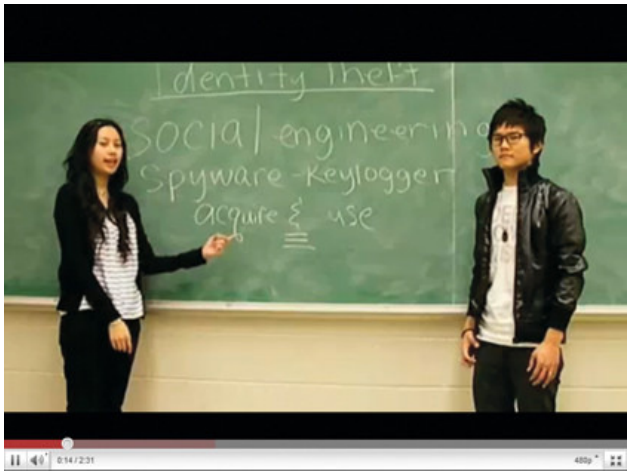
The *Japan Times* first reported the problem back in 2003. In that year alone, 2,768 victims parted with 2.26 billion Yen (about £17 million).

Social engineering is a kind of oil that lubricates the wheels of many online scams, from phishing to Ebay cons. By crafting a situation to appear as authentic and as urgent as possible, such techniques can be used to get whatever you want, and this extends to gaining physical access to areas from which you might otherwise be barred.

The key is to appear as if you're supposed to be there by preying on the assumption of others.

**Direct access**

The simplest method is simply to tailgate someone. That is, to have someone hold an otherwise secure door open for you while you follow them through it on the pretext of having left your security pass inside.




A classic method of carrying out this attack is to find out where a company's smokers go to indulge in their habit. Simply hanging around holding a lit cigarette (no need to inhale if you don't smoke) can be enough to establish you as someone with a right to be there.

When someone makes a move to return to the building, simply patting your pockets, uttering an expletive and asking if they can let you in is usually enough to gain access. The lesson here is never to let anyone into a building who isn't personally known to you.

**Give and take**

Another social engineering attack, called a quid pro quo (Latin for 'something for something'), can offer instant access to a company's systems, passwords and other information – as long as the attacker seems to be giving something in return.

A very popular form of this attack is common in the US. The attacker, having discovered the range of direct dial numbers for the target company, will call each of them in a random order under the pretext of being from the IT department and returning a call to the help desk.

The idea is that eventually he'll stumble on someone who really does need help with an IT problem. The victim is more than happy to do whatever the caller says in exchange for the quid pro quo immediate fix – including turning off antivirus protection, then downloading and installing malware to their PC in the guise of setting up software patches.

Weeding out social engineers from legitimate callers is simple. The golden rule is: if what you hear seems too good or convenient to be true, it usually is. If you're in any doubt that you're dealing with a legitimate caller, especially if you received the call unexpectedly and the person at the other end is demanding a high level of personal detail, don't become angry or abusive, especially if you have caller ID and the caller has withheld their number.

A better idea is to say you're busy, ask for a phone number and say you'll call them back at a time convenient to you. If the person at the other end is making a legitimate enquiry, he or she will be more than willing to give you their contact details and a problem number as a reference. If the caller makes excuses, or insists on the required information being given immediately, you know you're likely to be talking to a social engineer.

In situations like this, state your suspicions calmly and clearly, then wait silently for a reply. It's likely that the line will go dead as the scammer realises that the game is up.

---

First published in PC Plus Issue 301

Liked this? Then check out Who's hacking your PC?



Tags: social engineering, online scams, online fraud



## Tell us what you think

You need to Log in or register to post comments