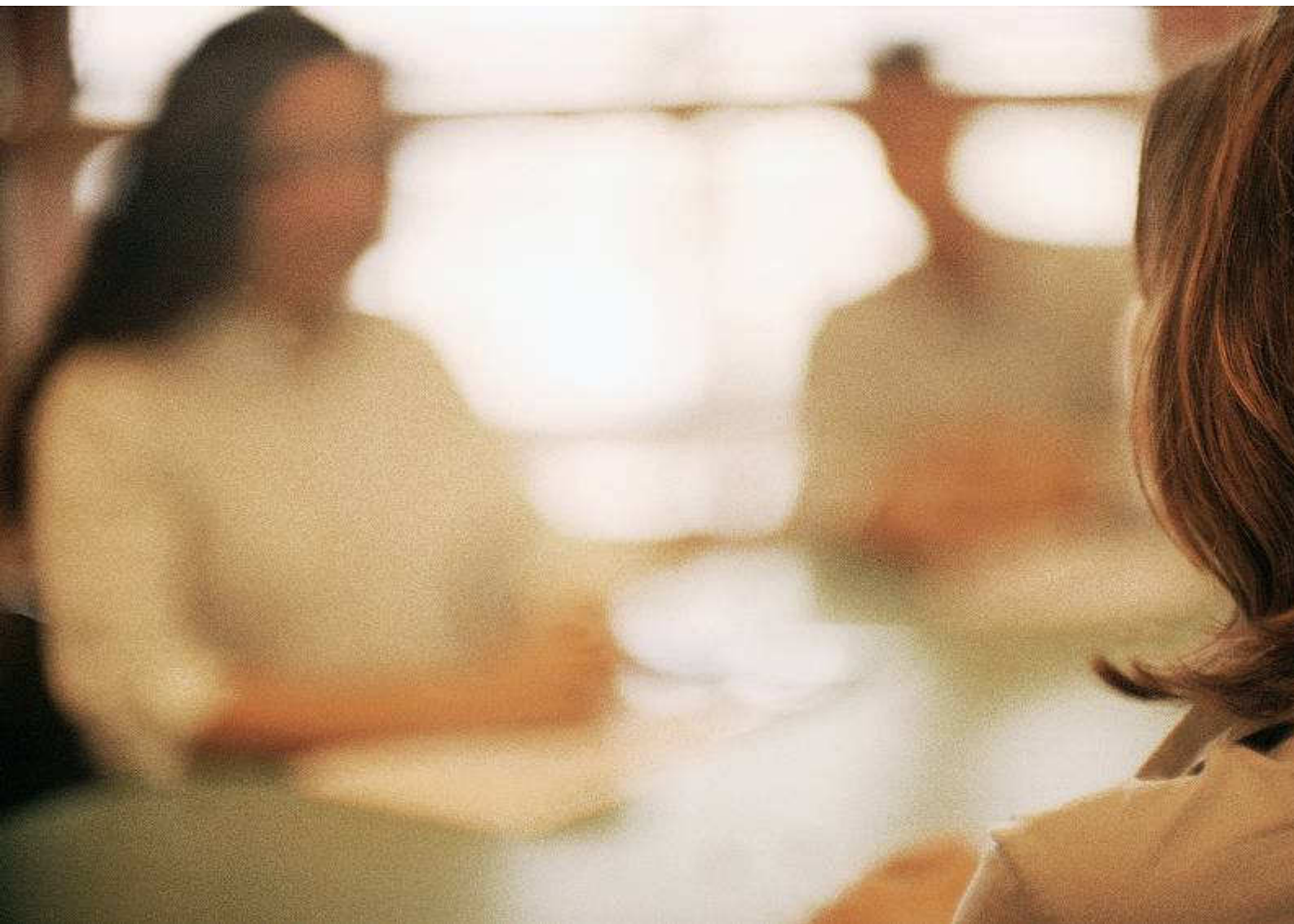




SAFECOMS

Social Vulnerability Testing



As technical defences against Internet based attacks become more sophisticated, professional hackers are turning to the exploitation of human weakness as an alternative (and easier) method of gaining unauthorised access to systems and information. This form of attack – generally referred to as “social engineering” – bypasses your entire investment in technical security controls.

More and more of our clients are therefore testing the effectiveness of their security defences by using our dedicated service to simulate social engineering attacks; the results of which provides management with an accurate and comprehensive picture of the ‘human’ vulnerabilities in their organisation.

Testing The Human Factor

- Your IT Helpdesk team have detailed procedures about password resets - but do they always follow them when under pressure? Our testing attempts to steal a user's electronic identity through a series of phone calls to the helpdesk – and finds out just how robust those procedures really are.
- You have information classification policies in place, and there are shredders located throughout the building – but do staff dispose of confidential documents properly? What sensitive information can be gathered by rummaging through your rubbish sacks?
- Your employees have been told about the importance of keeping their passwords secure – but has the message really sunk in? How many of your staff will reveal their passwords to a stranger over the phone, or will fall for a “phishing scam” based on a spoof email?
- You have invested significant sums in electronic swipe card systems and other physical security features – but will this investment actually pay off? How easy is it for an attacker armed just with a clipboard and a bit of banter to wander into secure areas and roam around at will “checking compliance with fire regulations”?
- Staff in your customer contact centre have been briefed on fraud prevention – but they've also had the importance of being “customer friendly” and demonstrating a “can do” attitude drummed into them. Which of these potentially conflicting messages will prevail when they are faced with a cunning caller attempting to obtain information about one of your customers in order to steal their identity?

Methodology

When carrying out social vulnerability tests Safecom's consultants follow a mature and proven methodology – using exactly the techniques used by real attackers. The exact scope of each test is dependent on your organisation's particular concerns, but typically this is a two phase process:

- i. We gather as much information as possible to build a picture of the organisation, the people who work in it, customers, the IT infrastructure, and possible points of weakness (both physical and logical)
- ii. We construct "attacks" based on that information – these are aimed at obtaining employee's network log-on credentials, obtaining confidential or sensitive information, gaining physical access to "secure" areas, and gaining sufficient information about selected customers to facilitate identity theft.

Social engineering is by definition opportunistic; the gathering of a single unexpected piece of information can cause the attacker to re-focus their approach in an entirely new way. If a social vulnerability test is to be of real value, it needs to be as authentic as possible and therefore follow the opportunistic course of the real life attacker.

Information Gathering

We commence testing, by gathering information about the company, its employees and customers from a variety of sources. Typically these will include

- **The Internet:** searches using tools such as *fingergoogle* can bring up useful information about the organisation, such as emails sent by employees to technical forums, biographic notes of senior employees who have spoken at conferences etc.
- **Rubbish:** many organisations store their rubbish bags in easily accessible places. The contents of such rubbish often provides valuable data for the attacker. For example, a past rubbish search by Safecom's revealed a list of all change management items currently in progress within the client's IT Department. It included the name of the staff member working on the change as well as the contact details of the internal "client": such details provide significant scope for informed fake phone calls to those internal "clients" posing as a new colleague of the relevant IT staff member.
- **HR:** many organisations now advertise job vacancies on their website, often with a specific contact person in HR who can be called for further information. Posing on the phone as a



prospective job applicant, significant useful background information can be unearthed from the HR team (who are, of course, trying to be helpful).

- **Reception:** as with HR staff, receptionists are generally instinctively helpful and try to assist callers however they can. By posing in a variety of roles, valuable information can usually be obtained from this source about the organisation, individual staff members, departments, the physical layout of the building and so on.
- **IT Department:** most IT staff enjoy the opportunity to talk at a technical level about what they have built and implemented in their workplace: we exploit this natural enthusiasm by posing over the phone as, for example, a student researching into “best practice” in enterprise IT architecture.

Attacks

Results gained from the information gathering phase provide us with ‘leads’ which we use to construct attacks. The exact forms of attack are many and various, and are best illustrated by a real “attack” recently undertaken by Safecom for a major financial services organisation (names have been fictionalised for obvious reasons).

ANATOMY OF AN ATTACK

Objective: To take over the network identity of a user by getting the helpdesk to perform a password reset

Define Target: looking for a senior PA (generally they have access to confidential folders on the network), ideally one who is a recent hire and therefore less well known to helpdesk team

Find The Target: phone call to reception posing as someone from the organisers of the “UK PA of the Year Awards” seeking possible nominations. Found out names, roles and direct contact details of all senior PAs, and that “Sally” had only recently started.

Learn About Target: still using the “UK PA of the Year Awards” subterfuge, speak to “Sally” and find out useful background information about her – location in the building, that she started 2 months ago, that she works alongside “Anne” (another senior PA), etc.

Research The Helpdesk: phone call to reception posing as someone from the “Helpdesk Association” organising a conference for helpdesk professionals. Found out phone number of helpdesk, name of manager and ascertained that it was staffed 24x7.

Go For The Kill: Called the helpdesk posing as “Sally”. Complained that locked out of computer, desperate as had important document to get out in next 30 minutes, asking for password reset. Helpdesk breached its own procedures and reset password based on “validation” of identity from basic background information already obtained about “Sally”. Using Citrix remote access set up, able to log onto network as “Sally”.

Physical Safety

As well as determining their susceptibility to electronic identity theft, organisations often ask us to test the effectiveness of their physical security.

In particular, many organisations regard the physical location of certain functions within their building as sensitive information; attempted assaults by disgruntled customers or others who believe they have been wronged in some way by the organisation are an increasingly common phenomenon. Organisations have a duty of care to provide a safe workplace for their staff, and it is therefore important that they determine how difficult or easy it is for an outsider to identify the physical location of a particular function (e.g. debt recovery) within an office building, and to then gain physical access to that location.

Additionally, gaining physical access to server/comms rooms where critical systems are kept is a common objective of a hacker. The scope of social vulnerability tests therefore typically includes attempts to socially engineer physical access to sensitive locations. We do this using a variety of subterfuges, ranging from “tailgating” of staff, posing as a visiting technician or building maintenance worker, or making a “personal delivery” to someone in a sensitive position.



Outcomes – Improved Security

The overriding objective of a social vulnerability test is to provide an organisation’s management with an authentic view of security weaknesses that need to be addressed. This information can then be used to plan targeted training initiatives and policy and procedure reviews.

Training programmes based around actual events discovered during the course of a social vulnerability test are far more effective than those based on abstract examples of incidents that have reportedly occurred in other organisations. Such an approach automatically pre-empts the “that would never happen here...” school of complacent thinking.

A well executed social vulnerability test (particularly where the results are presented back to senior management and staff) also plays an important role in reinforcing the fact that information security is not just “an IT thing”; rather it is something that everyone plays a role in. It emphasises that “security” needs to be viewed as a core part of corporate culture - in much the same way that customer service and innovative thinking are.

Find Out More

For a confidential discussion about Safecom’s social vulnerability service please contact us:

Phone: 01223 576044

Email: info@safecom.co.uk