IT Security Awareness Training

IT security these days is an issue for all members of staff in your company, not just dedicated IT security staff or IT support personnel.

By Robert Schifreen

The Internet has changed the way we do business. But it has also changed the way that computer systems get misused. In the early days of big databases, hacking into the system meant dialling a dedicated modem (often at international rates) and guessing passwords. Now, breaking into a system means doing an automated Internet search for servers without the most recent service packs. An entire industry has sprung up to help companies protect Internet-facing systems from abuse. However much money you have available to spend on IT security products, you can guarantee that you'll have no trouble finding people to take it from you. There are organisations queuing up to sell you firewalls, intrusion detection, access control, virus scanning, managed firewalls and much more.

And there is no shortage of training organisations to help IT security staff understand the techniques and practice of securing the machines - which is a jolly good thing, because configuring and maintaining a firewall is not something that just anyone can walk into. It's a skilled job, and one that can spell disaster if it goes wrong - because, if something is wrong, the first you'll know about it is when your company's private documents turn up on a hacker Web site.

It's impossible to run any company nowadays without embracing the Internet. The myriad potential problems and security implications must be looked upon as a necessary evil. Take the WHOIS system, for example. It allows you to find out the contact details of the person who has registered any Internet domain. Think of a company name, and type its domain name into a WHOIS lookup server. You'll get back the name and telephone number of the "administrative contact" - ie, the person within that company who made the registration. So why is this a security risk? Because of a hacking technique called social engineering. This involves techniques such as telephoning an end-user within a company and trying to con them into divulging their password.

Social Engineering

The classic method is to pretend that you're calling from the user's IT support department, and would they be interested in testing a new version of the in-house database software? All you'll need is their ID and password and you can upgrade their account right away. But when you call the unsuspecting user, who should you pretend to be? Ideally, someone from the user's company who is senior in the IT department. And, hey presto, the WHOIS database gives you just that. Which is why I always advise companies to use a false name when registering domains, and to inform the switchboard people where calls for that particular "person" should be directed.

There are hundreds of ways of breaking into systems. Some of them require technical knowledge, while others rely more on the perpetrator's social skills. But when we think about computer hacking in the Internet age, we often overlook one crucial point. The nature of the human target - ie, the person on the receiving end of the attempted hack - has changed. Once upon a time, targets were security managers, database administrators and so on - but not any more. Now, the typical route into your company for a hack, virus, or other unwanted effect of the IT age, is via the end-user.

Security companies tend not to bother talking to end-users. After all, end-users aren't the people who hand over the money for a new firewall. And end-users don't really care about IT security anyway. Why should they have to? Their job is to sell products, or write brochures, or type letters. They use a computer because they are told to and because it's faster than a typewriter. Why should they have to care about minimum password lengths?

Security awareness training is the art of making them care about, and be aware of, such things. If you don't, and if your end-users become the target of internal or external hackers, your company is at risk - and often in ways that no firewall or other traditional IT security product can prevent. Your ultimate goal in all this is to make end-users think about security all the time. Whenever they change their password, or install a new program, or take a laptop home etc they should think about the security implications of doing so.

Your most important weapon in the battle to make this happen is the IT security policy. This is a written document that tells staff what they can and can't do. For example, they must change passwords every month and not write them down, and all laptops taken offsite must use encryption and not be left unattended in cars.

Explain To Users

Just as important as the content of the policy, and maintaining it properly, is how the document gets "sold" to users. Rules are made to be broken, and rules which appear to be pointless or most unfairly implemented are those which get broken first. So an IT security policy should not simply be a list of meaningless rules which every new joiner is forced to read and sign. By all means have a "no passwords with fewer than eight characters" rule, but also explain why. Tech support and security staff know all about dictionary crackers and brute-force tools, but the average secretary does not.

Wherever possible, sprinkle your explanations with anecdotes. These can be taken from personal experience or from newspaper or Web archives. Citing a real case helps to make the theoretical seem more real. For example, my favourite anecdote regarding a hard disk that broke and which was not backed up involves a company which installed thousands of condom vending machines around a particular country. Without access to the database of locations, they had no idea where the machines were and so could not collect the cash or re-stock them. They eventually recovered their database with the help of a specialist data recovery firm, albeit for a very high fee.

Training

Ideally, all end-users should receive some simple training in IT security awareness. That means all non-technical staff, from post room assistants to board-level directors, as well as inexperienced tech support staff. This is best done as a formal training course, but if time or budgets preclude this then a circulated Word document or some pages on the intranet can substitute. The remainder of this article highlights some of the most important points that you should stress to your users.

Safe Data

Everyone knows that data being lost or corrupted is not good for business, but explain this further. Explain all the different types of data that the company creates and processes, and illustrate the sort of damage that loss, corruption or leakage of each type would do (or, just as importantly, would not do). For example, if details of the food on offer in the canteen were to be leaked to competitors, it wouldn't do any harm. But if details from the salaries database were leaked, it would allow competitors to poach existing staff without paying too much over the odds. Other types of data which need to be discussed include new product ideas, suggestions from staff on how to improve things, correspondence, costings and budgets, customer lists, marketing plans etc. Of particular interest is the file of customer complaints - anyone who knows what people don't like about your company can then do it better.

> *"These days, the typical route into your company for a hack, virus or other unwanted effect of the IT age, is via the end-user."*

Accidents Will Happen

Everyone knows that accidents do happen. You have to allow for this, to a certain extent, and there is no harm in telling users that this is the case. Dismissing someone for accidentally sending an email to the wrong address or formatting the wrong floppy disk does no one any good, assuming that it's not a regular occurrence. Assuming your backup strategy is correct, the actual effects of a file being accidentally deleted should be minimal anyway, so don't be afraid to tell users that you are willing to tolerate occasional accidents.

Talk And Dive

Not all security breaches take place in an office and involve a computer. How many times have you sat on a crowded train or plane and overheard company executives talking about private matters? Make staff aware of the dangers of doing this, by example or extrapolation.

Also cover the topic of dumpster diving, where people rummage around in trash cans outside office buildings in order to look for confidential printouts and other documents that have been thrown away. One favourite example which I personally encountered some years ago was the company which had thrown away a printout of the salary spreadsheet for the entire company. The document had been shredded into strips, but had been placed in the shredder the wrong way round, so each strip was a complete, perfectly legible row of the spreadsheet, containing an employee's name and salary details.

Password Compromises

Everyone knows the standard rules about not sharing passwords. Most companies have security policies which simply state that it's not allowed. However, in the real world things aren't always so simple. Sometimes, cases arise that cause a dilemma for a staff member. For example, he or she may be asked by a superior to allow a password to be shared. What should the employee do? Clearly, you want them to refuse. But how? Awareness training means pre-arming employees with a suitable excuse such as having been told by someone even more senior that this sort of thing must never happen. This is just one reason why any security awareness training programme needs management buy-in at the highest level. It's also a good idea to tell staff why lending their password to another staff member is so unwise. Point out that any actions taken with that password will show up in the log files under the name of the password's owner.

On the subject of log files, most staff are aware that their computer (and especially Web) access is logged. Most feel that this is an invasion of privacy, and will resent it (either silently or vociferously). Security awareness training gives IT staff and senior managers a good opportunity to justify the use of such techniques. Stress the good points, such as being able to stop viruses before they reach the recipient. Sending a virus to a client is not good for business. And stress that preventing access to things such as pornographic Web sites is essential because, if it goes on, this could lead to prosecution of the company's directors.

Suspicions

It's important to lay down some guidelines about what to do, and what not to do, if a staff member suspects that a colleague is misusing the computer system for personal gain or simple malice. Despite the reputation of the Internet as being home to millions of hackers, the majority of computer misuse is still perpetrated by current employees of the victim company. Sometimes it is for reasons of greed or malice, but sometimes the employee is being bribed, blackmailed or conned.

This session might also be a good time to remind users that the PC on their desk and the data it contains belong to the company and not to the users. So, within reason, anything the company wants to do with that computer, they are quite entitled to do. Though it helps if you put a gentler spin on the explanation!

> *"Your ultimate goal in all this is to make end-users think about security all the time."*

Homeworking

Staff who work from home pose a unique security risk, and this needs to be managed. The way you do this will depend to a certain degree on whether they take their desktop or laptop home from the office, or whether they take files away to access on their own PC at home. If the work is done on a company-owned PC, you have more right to say what can and can't be done on that machine when it is off the premises. Make it clear that there is a different set of risks associated with home-based PCs compared to those used at the office. For example, Microsoft's main systems were hacked late last year and, according to Microsoft itself, the hackers managed to access such crucial files as the source code for future versions of Windows. Current understanding is that the hackers got into the Microsoft network via the home machine of a programmer, on which they had managed to plant a trojan.

Misaddressed Mail And Spam

Explain that, sometimes, email gets wrongly delivered. And also explain about unsolicited email, or spam. Having explained what these things are, continue by explaining what to do about them. And, most importantly, justify your reasoning. Misaddressed mail should be deleted or forwarded to the IT department. It's best not to return it to the sender, as this can involve you in arguments - especially if the mail was of a confidential nature. If you regularly receive misaddressed email from one particular location, consider mailing the postmaster at the sender's domain to explain what's going on. Users need to be told, strongly, never to reply to spam. Replying to such messages highlights the user's email address as a "live" address, and will simply result in even more junk mail. Delete the messages, or forward them to the IT department. Don't bother moaning to the postmaster of the sender's domain - thousands of other people will have already done so.

Viruses, Hoaxes And Trojans

A decade ago, most viruses spread via infected .EXE files or bootable floppies. Nowadays, they spread mostly via Outlook. An infected message might contain a script file which sends a copy of itself to the entire contents of a user's Outlook address book and then formats the user's hard disk. Not only does the user suffer, but all of his or her contacts will suffer the same fate - assuming, of course, that they click on the attached script file in order to run it. If they don't, the virus does nothing. It is crucial to explain the importance of not running any email attachments. This should also be extended to any executable file. Ironically, when the Love Bug virus hit computers around the world last year, many of the people who clicked on the attachment and allowed it to spread were IT staff who should have known better. In many cases, non-technical end-users were, quite rightly, suspicious. Incidentally, there are numerous ways of bypassing the effects of the Outlook security updates which are supposed to restrict users' ability to send and receive attachments. You should explain to users precisely why bypassing this restriction is a bad idea.

In addition to covering viruses, be sure to mention hoaxes and trojans. Hoaxes circulate on a regular basis, and take the form of warnings about particularly nasty viruses. The recipient is advised to pass on the warning to all of his or her contacts. This simply clogs up internal mail servers. Make sure that staff know they should never send broadcast mail to the entire company except in grave emergencies. Instead, pass the suspected hoax to the IT department, who can check on the Web sites of reputable anti-virus companies who will generally know whether the warning is genuine.

Conclusion

Any company which treats IT security as being of relevance only to the IT department will not survive for long. Hackers no longer target just IT staff, but prefer to attack via end-users. So it is crucial that all users are aware of how to recognise the signs and what to do about it. Not only will this help your organisation survive an attack, but it will also help to improve staff morale by making them feel more valued. While thinking about implementing a security awareness training programme for end-users, don't forget to consider training new IT support staff in a similar manner. For example, support staff are often the first point of contact when a user loses or forgets a password. But if a junior support person receives a call from a person whose voice he does not recognise, claiming to require his password to be changed, would the support person know what to do?

> *"How many times have you sat on a crowded train or plane and overheard company executives talking about private matters? Make staff aware of the dangers of doing this."*

PCSA

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.