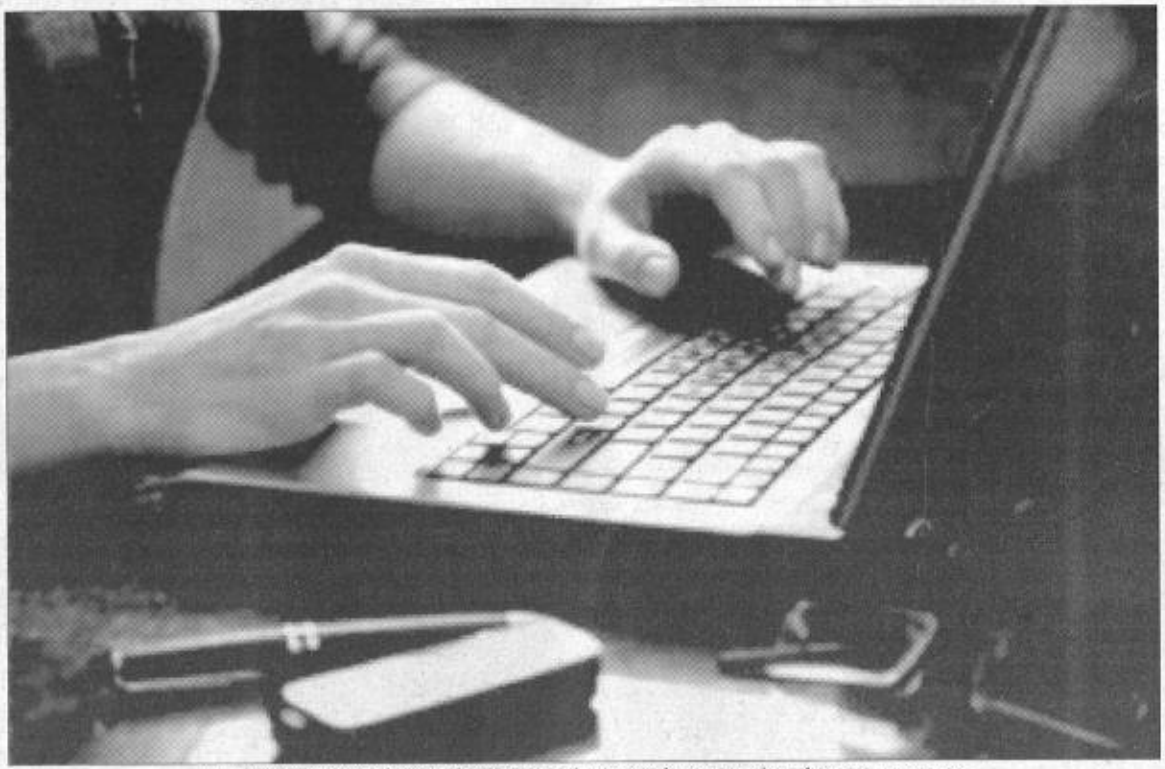
The risk of cyber crime to you and me

IN TODAY'S WORLD, THE REALITY IS THAT all individuals and organisations connected to the internet are vulnerable to cyber attack.

The number, type and sophistication of attacks continues to grow, as the threat report published last month by the Australian Cyber Security Centre (ACSC) points out.

It's not only large organisations that are under threat. Individuals or organisations that don't believe they have much to offer hackers can still be targeted. So even if you think you're a small target, you might still be at risk.



Many people mistakenly believe that hackers have nothing to gain from copying their information. Thinkstock

Illusion of trust

Malicious individuals and groups thrive on gathering information that can be used to enhance their attack strategies.

Hackers are becoming more focused on spear-phishing attacks, which are tailored to individual people, and any piece of information about you can be of help.

Key to the hacker is the issue of trust. The information gathered is used to build a profile of the target with the aim to have enough data that allows the hacker to appear trustworthy.

In most cases, the hacker will attempt to impersonate an entity that is trusted by you. The more information the hacker has on you, the more likely they will be able to maintain the illusion long enough to achieve their aims.

The effects of a successful attack vary significantly, largely depending on the motivation of the hacker.

For most of us, identity theft is likely to cause the most damage because it badly impacts on our ability to go about our normal daily life. Our credit rating could be severely compromised, for example.

To make matters worse, the process of addressing the damage of an attack can be costly, time consuming and emotionally exhausting.

In other cases, the damage could be in the form of confidential information, such as medical history records, ending up in the hands of malicious parties, thus making you susceptible to different kinds of blackmail.

The recent breach of the Ashley Madison website is a typical example of confidential information about individuals that could be exploited by malicious parties.

Your access is important to hackers

But specific personal information is not the only driving factor behind cyber attacks. Often, the resources or the access you have to other systems is the overall goal.

A common misconception held by many individuals and organisations is that if they do not have anything of value on their systems, they are not likely to be attacked. Or the hackers have nothing to gain from copying all their information.

The information value may be zero, but the resources are precious commodities which can be easily used in two ways:

> to launch more intensive, distributed attacks on the hacker's primary target;

> they can be "leased out" in the form of botnets to other parties.

From the point of the user clearance, hackers again can exploit the knowledge about the target to attempt to gain access to systems that are difficult to reach.

Food for hacking thought

I was told of one case in the US where foreign hackers used the eating habits of the staff of a government organisation (obtained from credit charges) to launch a "watering hole" attack.

The hackers were able to easily compromise the server hosting the website of the restaurant frequented by the government employees, and they replaced the original PDF menus with a new set that had malware embedded in them.

Thus, when the government employees were viewing the menus from their secure machines, they were downloading the malware as well.

These are just some of the ways hackers can take advantage of the information gathered from attacks.

Unfortunately, the only limiting factor is the creativity of the malicious party. And hackers are very creative.

ABC