SNOOPING

Published in Silicon Times, October 2003

It's a general human tendency to have curiosity in the matters totally irrelevant to them. And when it comes to the Internet, this tendency always multifold

Have you ever felt that you're being monitored? Your computer usage in particular: by your parents or employers or by some unidentified stranger. If your answer is yes then you know how troublesome it is to part with one's privacy. If you say NO (Are you sure?), better be alert.

Is it not a matter of concern to know that your associates: parents, boss, government and law enforcing agencies included are all preparing to poke into your inbox, browser and your computer? They may have their own reasons for doing so but ultimately it's your privacy that's being ransacked. And the above process is called snooping.

Snooping refers to the act of unauthorized access to others database and personal information. It also covers the act of parting with confidential information (such as customer's data) for the benefit of a third party.
Unlike its relatives-cyber stalking, cyber crime etc, snooping may not have criminal impact or assault, but nevertheless loosing one's privacy can be equally disturbing.

There are many reasons to poke and snoop around.

Curiosity - "hum... what is that IP?"
Security - "hum... why is that IP in my firewall logs?!"
Curious programmers may have their own reasons "HUMM... Me? The 007 INTERNET SPY!!"
Inside the office-"Is that man working for my company or chatting with his girlfriend using office PC?"
Corporate intelligence-"At what rate my competitor is bidding so that I can undercut his quotation?"
Whatever your cause, be prepared to answer questions if someone traces your phone number from the IP you left on their logs...

Snooping in Office

Most employees protest against cyber snooping, but employers are firm on their stand and justify their action. Would you be comfortable if your company pries into your mail on the pretext of productivity?

It's no more a secret, nor a surprise that companies have arrangements to monitor their employee's computer usage- particularly the internet. The Internet has changed the cultural mindset of many. At one time, indulging in office gossip at the canteen or the smoking bay may have been the favorite passtime of office goers. Today, chatting online and browsing through the Net have become the new favorite activity, eating into employee productivity. Reason enough for employers to monitor the Internet access of their employees. Many companies now impose a restriction on Internet access or monitor Internet usage with the stated objective of increasing productivity and work output.

Apart from blocking sites, companies can also restrict certain services. Protocols such as FTP or Socks, which are generally used for file downloads and instant messaging, can be disabled. Some companies use dedicated firewalls for this purpose. This may reduce the Net congestion that takes place due to downloads or chatting, allowing the employee to browse the web at the same time.

Employers snooping into an employee's email are a rare case. In most cases there'll be some filtering software which automatically blocks and sends back messages having certain key words such as "sex".

According to the Electronics Communication Privacy Act of US, employees have limited privacy rights when it comes to official mail. But various organisations are fighting for privacy protection. The police have to obtain warrants to tap telephone conversations or steam open mail. Similar restrictions would be placed on employers in relation to e-mails sent by their staff.

But in India, in spite of the new cyber law, there exists no law which draws a line between privacy and security issues. As a result, there are no rules for cyber snooping by companies. But to be on the safer side, it is the company's obligation to verify all legal aspects before getting into employee snooping.

Of course, for every site that's banned, there are ways to get around it.

Blocking sites may not solve the problem. Creating awareness about the problems faced and instilling a balance between productivity and entertainment seems a better option. Monitoring also raises the issue of democratic decision making.

After all, who decides what is good and what is bad? Open discussions and debates on such issues are therefore considered more efficient than blocking just about every site in sight.

Some of the employee monitoring softwares:

SuperScout, CyberPredator, WinGuardian, IWarden, TaskGuard2000 etc.

Competitive Intelligence

Corporate spies come in many guises, but they all have one thing in common: They want to use a company's secrets for competitive gain.

Consider these 2 examples:

1. An engineer regularly had lunch with a former boss now working for a competitor, and he fancied himself a hero as he collected rewards from management for gathering competitive intelligence. Little did he know that the information he was giving up in return caused his employer, formerly the market leader, to lose three major bids in 14 months.

2. Immigrants from Eastern Europe who were working as scientists on an American defense project kept getting unsolicited invitations from their home countries to speak at seminars or serve as paid consultants. The invitations appealed to them as scientists—they wanted to share information about their work with peers. The countries saw this kind of intelligence gathering as cheaper than research and development.

Because most organizations don't have a means of tracking the loss of proprietary information; they go on constantly hemorrhaging, constantly losing market share. Gradually it takes the vitality out of the organization because it's hard to invent and create things faster than people are leaking it or stealing it. It might be seen as, but can’t be ignored as “just bad luck in business”.

Fortunately, hanging onto proprietary information—whether it's a trade secret or just a few strategic details that may seem inconsequential—isn't just about luck. It's about understanding the dark forces that are trying to get information from a company and piece it together in a useful way. Some of these forces come in the guise of "competitive intelligence" researchers who, in theory anyway, are governed by a set of legal and ethical guidelines carefully wrought by the Society of Competitive Intelligence Professionals (SCIP). Others are outright spies, hired by competitors or even foreign governments, who'll stop at nothing—bribes, thievery, a pressure-activated tape recorder hidden in the CEO's chair and so on.

But it's bad luck that adds up to billions of dollars each year for U.S. businesses, according to a survey done by the American Society for Industrial Security. The 138 companies that responded to the September 2002 survey reported that the loss of proprietary information, often in the form of research and development or financial data, cost them at least $53 billion in 2001 alone.

Online Privacy

Watch out: the e-mail entering your inbox might be loaded with software that lets marketers track your moves online, and you may not even be aware that you've been bugged.

Almost all Web sites plant bits of code called "cookies" on consumers' hard drives for regular invigilation of Internet pages for returning visitors and better target ads. Now, enhanced messages that share the look and feel of Web pages are being used to deliver the same bits of code through e-mail, in many cases without regard for safeguards that have been developed to protect consumer privacy on the Web.

However cookies can’t be a serious threat to your privacy since they can be barred. Some e-mail programs already include settings allowing consumers to block cookies. Microsoft's Internet Explorer 6.0, for example, offers controls for cookies on the Web and via the company's Outlook and Outlook Express e-mail programs. Turning on the "prompt for cookies" setting can reveal the stunning extent of the problem, unmasking unsolicited HTML e-mail messages that try to lay down cookies on a hard drive.

Have you experienced this? You buy a mobile connection filling a form containing your personal details. Within hours of activation of your connection, the first person to call you on your mobile will be none other than a salesman or insurance advisor or a marketing representative. Ask him from where he got your number and he’ll hang up. You need not wonder! It’s a part of “terms and conditions” that your cell operator (or any other business firm for that matter) insist that it’s entitled to use your personal information.

To be sure, some retailers are starting to refer to e-mail monitoring in privacy policies. Amazon.com, for example, mentions that it may use tracking methods via e-mail to determine preferences for future communications. Still, privacy advocates said e-mail privacy practices are largely under-disclosed compared with other media such as the Web.

Well. For all the bluster about online privacy, most of us don't care that much. Consider:

1. AmericanGreetings.com, a top-20 Web site, has a privacy policy click-through rate of just .009 %(i.e. % of people going through its Privacy policy while signing up). So low it's barely statistically significant.

2. E-tailers such as LLBean.com, Ticketmaster Online-Citysearch and Bloomingdales.com tell you right up front that your data is given to partners. And people buy things from them all the time.

3. About.com ranks as the seventh most popular Web site, logging 50 million visits in August. But only 20,550, or about .04%, clicked on the company's privacy link.

Most of us are not serious about online privacy. Mainly because it hasn’t caused much damage compared to the impact of virus, cyber stalking and other dangerous devils of the internet. But the irritation and mental disturbance it can give can be equally severe.

Data Protection:

The importance of data privacy is growing. In the past, it was possible to maintain reasonable control over who could view data because access tended to be available only through individual systems and applications with a known set of users. Rarely was there a need to distinguish between those who could update data and those who could view it, as they were usually be the same people. As a result, security breaches were relatively rare.

But advances in technology have brought about new problems. Data can now be downloaded locally from spreadsheets and databases, various middleware products can transfer data between applications or to local datamarts, and data warehousing has made it possible to assemble data accessible by many people in an organisation. In most cases, these technologies were deployed without any thought about security.

The internet further extended the use of shared data through credit card details and e-mail addresses, and increased the importance of data privacy. Few people are happy at the idea of their e-mail address being freely distributed and everyone who enters their credit card details on the internet expects the information to be held securely. Will it be? Is the question.

Threats to data protection:

1. Destruction-physical destruction of vital information assets using conventional weapons.

2. Disruption-electronic disruption using non-conventional weapons, viz. EMP (electromagnetic pulse), DEW (directed energy weapons), etc.

3. Data manipulation-computer viruses, worms, Trojans, and other malicious software.

4. Data interception-sniffers and other 'snooping' techniques to intercept confidential information.

5. Chipping-malicious software embedded surreptitiously in systems.

Firewalls are what comes to one’s mind on the thought of security but a firewall, however, is not impregnable. There isn't a firewall that a group of experts can't get around, despite the increasing sophistication of firewall defenses. In the eternal war between hackers and defenders, the defenders have to be lucky all the time, hackers just once.

State sponsored Snooping.

Since past 3 years net service providers in the UK were obliged to carry out surveillance of some customers' web habits on behalf of the police.
Controversial laws passed in 2000 oblige large communications companies to install technology that allows one in 10,000 of their customers to be watched.

The controversial Regulation of Investigatory Powers Act was passed in October 2000 and gave law enforcement agencies sweeping powers to snoop on the electronic lives of citizens.

In simplest words it's the internet equivalent of a telephone tap.

It also demands that service providers start monitoring a customer within 24 hours of being told that the police or other investigation agencies want to snoop on them.

The information gathered about what people look at on the web, the content of e-mail messages and their phone conversations would be passed to the police or a government monitoring station.

The bush administration in U.S also has similar law in force, with an official purpose of monitoring terrorist activities. FBI (Federal Bureau of Intelligence) has its own infamous Internet surveillance program called Carnivore.

Conclusion

The positive aspect of Snooping can be as an anti-terror panacea to lawmakers, a way of increasing productivity for employers, and so on.

On the other hand it'll also enable people to steal critical information and data and spy out to name a few.

It's not possible to eliminate snooping completely. It also doesn't mean that you stay helpless while being snooped. Everyone can protect themselves to a considerable extent. All one needs to do is to adopt some simple practices.

The future of electronic communication now rides on striking a workable balance between giving crime-fighting tools to the government and privacy guarantees to netizens.

SHRINIDHI H
www.shrinidhi.20m.com