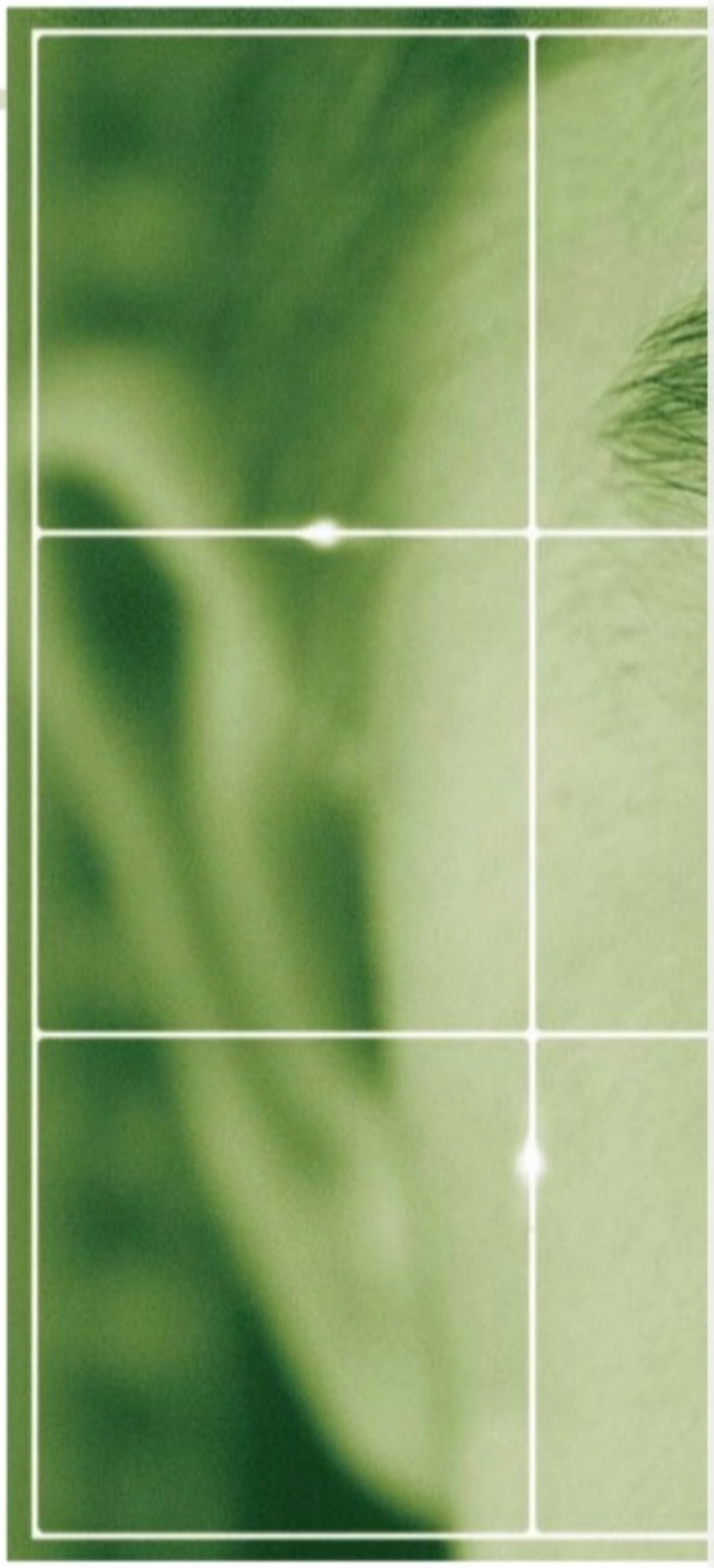
THE NAME GAME

AS ONE OF THE FASTEST GROWING CRIMES IN CANADA, IDENTITY THEFT IS BECOMING A SECURITY THREAT THAT EVERY COMPANY MUST UNDERSTAND, ADDRESS AND FIGHT.

By Jack Kohane



What's in a name? Whenever you sign a cheque, rent a car, mail a tax return, change your cell phone service provider or apply for a credit card, your name enters the public domain. Most of us don't give these everyday transactions a second thought. But not for the identity thief.

Called the cyber-crime of the 21st century, identity theft occurs when someone steals your personal information — such as social insurance numbers, driver's licence numbers, credit card and banking information, calling cards, birth certificates and passports — without your knowledge or consent, and uses it to impersonate you to conduct spending sprees, open new bank accounts, divert mail, apply for home mortgages, credit cards and social benefits, and business loans. All of it done in your name, and on your tab.

Obtaining confidential information isn't difficult. Called "dumpster diving," thieves will look through a business site's garbage for "pre-approved" credit card offers, copies of old bills and loan applications. They may overhear a person giving out personal information over a public telephone or cell phone, or peek over a person's shoulder as they use an ATM or fill out forms. They may telephone someone at your office and pretend to be a landlord, bank officer or employer in order to get confidential information. They may even use "inside" accomplices to steal files and laptops to access your company's information.

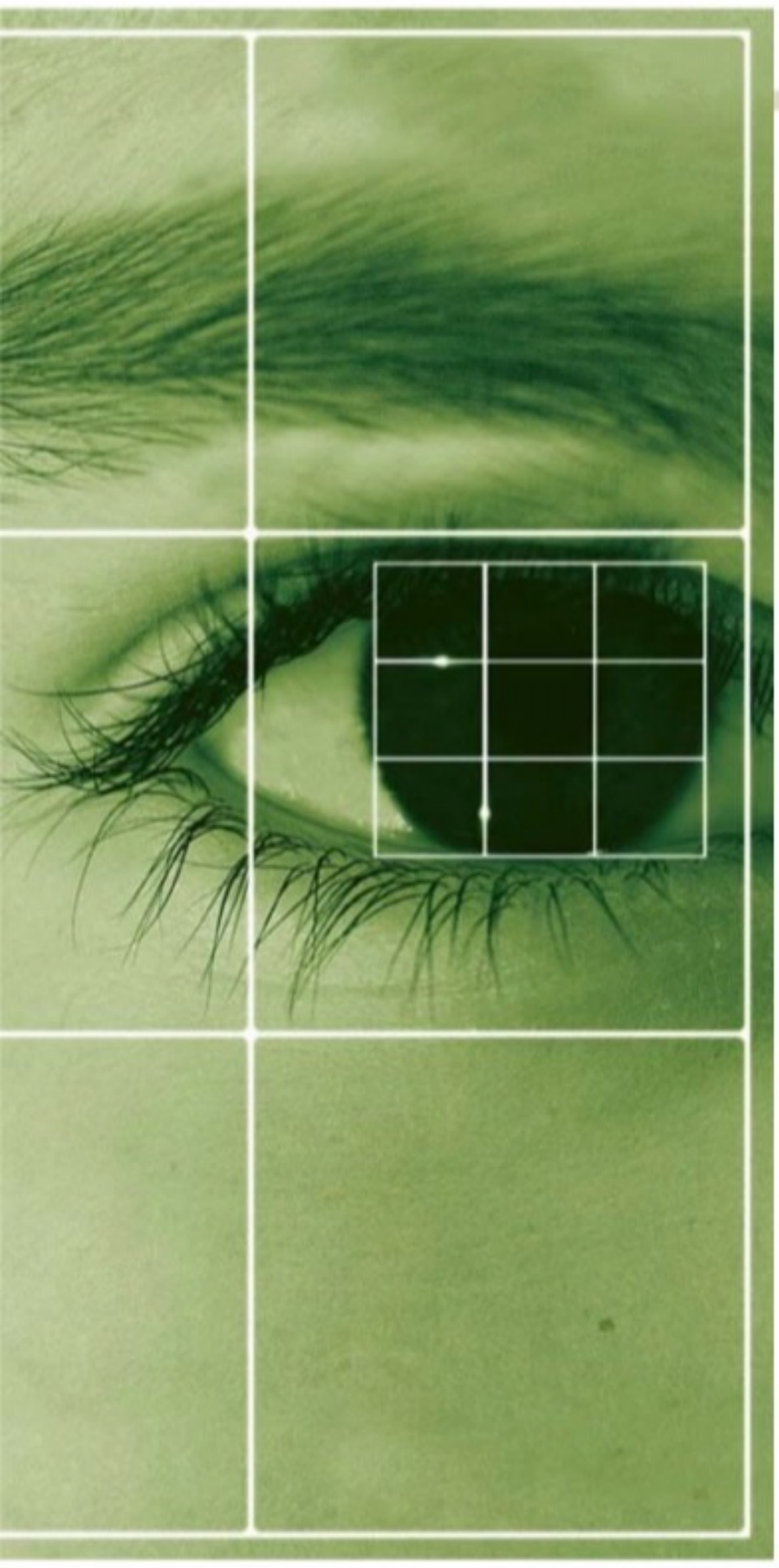
As more businesses use the Internet, new hi-tech methods are being harnessed by criminals to commit identity theft, including "phishing" which occurs when e-mails are sent to unsuspecting victims asking for information and providing links to false web sites; "pharming," arises when hackers exploit vulnerabilities in an organization's domain name system (DNS) server software and can target a financial institution's entire customer base through a Trojan program which embeds itself and waits for unwary victims to log on and perform financial transactions; and botnets (a.k.a. robot networks), strike when a hacker gains control of a PC or a network of PCs from a remote location after inserting a control program into an unsuspecting user's computer.

"Information is the elixir that drives identity thieves," says Ken Anderson, assistant commissioner of the Information and Privacy Commission of Ontario. "It's essential for companies to remember that privacy is not the responsibility of one division, department, branch, manager or executive. All businesses need to develop a culture of privacy across their organization's entire spectrum. Privacy is more than just an organizational contingency, it is a mindset — a way of thinking."

The Information and Privacy Commissioner of Ontario offers useful information tools and privacy management documents on its web site (www.ipc.on.ca) to assist companies in enhancing their privacy practices and policies through such means as: mapping data assets, carrying out privacy gaps, threat and risk analysis, conducting privacy impact and risk assessments, and executing a successful privacy strategy.

"This is a critical time for businesses to take the opportunity to review and improve their information management and security practices," remarks Anderson, adding that every enterprise should analyze its vulnerabilities, prepare a plan, implement policies and procedures that address technology, and continually evaluate and adjust that plan as technology advances.

Primarily perpetrated by organized crime and global terrorist organizations to raise funds, identity theft is now one of the fastest-growing crimes in Canada. The Canadian Council of Better Business Bureaus (CCBBB) estimated that in 2002, consumers, banks, credit card firms,



stores and other businesses lost about $2.5 billion to identity theft. In addition, two major Canadian credit bureaus, Equifax and Trans Union, indicate they receive approximately 1,400 to 1,800 identity theft complaints per month.

"ID thieves are getting more sophisticated, which means we have to combine all our resources to recognize, report and stop ID fraud," states Detective Inspector Scott Tod of the OPP Anti-Rackets Section and deputy director of PhoneBusters, a national anti-fraud call centre jointly operated by the Ontario Provincial Police and the Royal Canadian Mounted Police.

An expert in identity theft countermeasures, Brent MacLean, founder and CEO of J.B. MacLean Consulting and Wire Fraud Solutions in Toronto, points out the crucial signs that alert an organization to a breach of security: purchases not made that appear on the company's monthly bills; bills arrive on accounts the company doesn't own; a collection agency calls about unknown debts; credit card and bank statements that do not arrive; and denial of bank credit for reasons that do not match your understanding of your financial position.

BUILDING AWARENESS

To reduce a company's risk of falling prey to cyber-crime, MacLean recommends creating employee awareness about identity theft.

"Advise your staff never to give out sensitive company information to anyone who phones or e-mails unless they know who they are or can confirm that the person is from a legitimate company," he says. "Identity thieves may pose as representatives of financial institutions, Internet service providers and government agencies to get people to reveal vital information. Keep valuable customer data, such as credit card or bank account numbers, in a secure location in your business and not readily visible to others who may have access to the premises. Online businesses, which often depend on credit cards for payment, should consult the financial institutions with which they have merchant relationships to learn what programs or mechanisms may be most suitable for their business."

Building awareness amongst a company's personnel about the challenges of, and solutions to, identity theft can also be done via security-focused training sessions.

"To those people who value their jobs, highlighting the importance of security, clearly stating that it's more than just a corporate slogan, is very effective," says James Litchko, president of Litchko & Associates, an IT consulting firm in Kensington, Md., and past chairman of the IT Security Council for ASIS International, an organization of security professionals. "A training program must cover ways that allow employees to identify what information in the company is sensitive, and educating them about how to respond to people requesting employee contact or personal information. It's also prudent to shred all trashed corporate documents, and build a plan with your legal expert on how to respond if a loss or compromise happens."

Even though no security strategy can claim to be 100 per cent crime-resistant in protecting a company's physical and data assets, Anderson insists, "All of us must make the effort. Constant vigilance will reduce opportunities for identity thieves to make you a victim. Your customers entrust their vital information to you, so safeguarding that information the best way possible will ensure their ongoing trust and loyalty are kept." ■

Jack Kohane is a freelance writer based in Toronto, Ont.

CONSUMER ACTION

If you think you have been a victim of identity theft, there are steps you should immediately take to minimize damage and help prevent further fraud or theft.

Step one: contact each financial institution, credit card issuer or other company that provided the identity thief with unauthorized credit, money, goods or services.

Step two: contact Canada's two national credit reporting agencies, TransUnion Canada and Equifax Canada, and ask each agency to send you a copy of your credit report.

Step three: report the incident to your local police department. If a police report is available, include it in all your correspondence with financial institutions, credit issuers, credit reporting agencies and other companies.

Step four: report the incident to PhoneBusters' National Call Centre by calling 1-888-495-8501.

Following these steps can help prevent the imposter from doing any further harm, and start the process of clearing your company's name and reputation.

SOURCES

Information and Privacy Commission of Ontario • www.ipc.on.ca
J.B. MacLean Consulting • www.jbm.net
Litchko & Associates • www.litchko.com
PhoneBusters • www.phonebusters.com