Report on Phishing

A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States

Binational Working Group on Cross-Border Mass Marketing Fraud
October 2006

Report on Phishing

A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States

Contents

Executive Summary

Phishing refers to luring techniques used by identity thieves to fish for personal information in a pond of unsuspecting Internet users. It is a general term for the creation and use by criminals of e-mails and websites that have been designed to look like they come from well-known, legitimate and trusted businesses, financial institutions and government agencies. These criminals deceive Internet users into disclosing their bank and financial information or other personal data such as usernames and passwords.

Phishing continues to be one of the rapidly growing classes of identity theft scams on the Internet that is causing both short-term losses and long-term economic damage. In May of 2006, over 20,000 individual phishing complaints were reported, representing an increase of over 34% from the previous year. Recent data suggests that criminals are able to convince up to 5% of recipients to respond to their e-mails, resulting in an increasing number of consumers who have suffered credit card fraud, identity fraud, and financial loss. Estimated losses from phishing attacks are now in the billions of dollars worldwide, and those losses are growing.

Depending on the type of fraud that a criminal commits with the aid of stolen identifying data, individuals and businesses may lose anywhere from a few hundred dollars to tens of thousands of dollars.

Phishing also poses a particular threat because techniques used are constantly evolving. "Vishing," for example**,** involves identity thieves sending an e-mail designed in the same way as a phishing e-mail, yet instead of providing a fraudulent link to click on, the e-mail provides a customer service number that the client must call and is then prompted to "log in" using account numbers and passwords. Alternately, consumers will be called directly and told that they must call a fraudulent customer service number immediately in order to protect their account.

"Spear phishing" is a technique whereby e-mails that appear genuine are sent to all the employees or members within a certain company, government agency, organization, or group. Much like a standard phishing e-mail, the message might look like it comes from an employer, or from a colleague who might send an e-mail message to everyone in the company, in an attempt to gain login information. Spear phishing scams work to gain access to a company's entire computer system.

Phishing, like identity theft, is not confined to borders. Both Canada and the U.S. have undertaken a variety of initiatives and legislative reforms to combat phishing. Many of these initiatives are multi-sectoral, multi-jurisdictional and multi-agency, and extend beyond law enforcement entities.

In an effort to acquire a better understanding of the scope and magnitude of phishing, and the larger concept of identity theft, governments and the law enforcement community, with participation from the private sector, have established public reporting mechanisms.

Introduction

In October 2004, the Canada-U.S. Cross-Border Crime Forum released a report, prepared jointly by the U.S. Department of Justice (DOJ) and Public Safety and Emergency Preparedness Canada (PSEPC), on Identity Theft. The report identified, among other methods of committing identity theft, the growing use of a technique known as "phishing":

> Consumers will receive "spoofed" e-mails (e-mails that appear to belong to legitimate businesses such as financial institutions or online auction sites). These e-mails will typically redirect consumers to a spoofed website, appearing to be from that same business or entity. Similarly, many consumers receive "pretext" phone calls (phone calls from persons purporting to be with legitimate institutions or companies) asking them for personal information. In fact, the criminals behind these e-mails, websites and phone calls have no real connection with those businesses. Their sole purpose is to obtain the consumers' personal data to engage in various fraud schemes.[i]

The Canada-U.S. Cross-Border Crime Forum determined that it would be appropriate to follow up on the Identity Theft report with a joint report on Phishing and its impact on cross-border criminality. It directed the Canada-U.S. Working Group on Cross-Border Mass-Marketing Fraud, which reports to the Forum annually, to prepare this report. Prepared jointly by the U.S. DOJ and Public Safety and Emergency Preparedness Canada (PSEPC), the report is the result of contributions from the many agency and individual participants in the Working Group from the United States and Canada.

The objective of this report is to define the nature, scope and impact of phishing, to provide the public with information on how to respond to phishing schemes, and to identify current and promising approaches to combating phishing. It includes information on phishing trends, statistics and a discussion of the principal factors affecting the growing use of phishing by fraudsters.-

What Is Phishing?

The term *phishing* is a general term for the creation and use by criminals of e-mails and websites – designed to look like they come from well-known, legitimate and trusted businesses, financial institutions and government agencies – in an attempt to gather personal, financial and sensitive information. These criminals deceive Internet users into disclosing their bank and financial information or other personal data such as usernames and passwords, or into unwittingly downloading malicious computer code onto their computers that can allow the criminals subsequent access to those computers or the users' financial accounts.[ii]

Although phishing, identity theft and identity fraud are terms that are sometimes used interchangeably, some distinctions are in order. Phishing is best understood as one of a number of distinct methods that identity thieves use to "steal" information through deception – that is, by enticing unwitting consumers to give out their identifying or

financial information either unknowingly or under false pretenses, or by deceiving them into allowing criminals unauthorized access to their computers and personal data. The United States and some other countries use the term "identity theft," and the United Kingdom often uses the term "identity fraud," to refer broadly to the practice of obtaining and misusing others' identifying information for criminal purposes. Identity fraud also can be used to refer to the subsequent criminal use of others' identifying information to obtain goods or services, or to the use of fictitious identifying information (not necessarily associated with a real living person) to commit a crime.

Phishing is committed so that the criminal may obtain sensitive and valuable information about a consumer, usually with the goal of fraudulently obtaining access to the consumer's bank or other financial accounts. Often "phishers" will sell credit card or account numbers to other criminals, turning a very high profit for a relatively small technological investment.

The Scope of Phishing

There are no comprehensive statistics on the number of persons whose personal information is obtained through phishing schemes, or the total dollar losses attributable to phishing-related fraud. There are clear indications, however, that phishing has grown substantially over the past two years and has become a matter of concern throughout North America and other regions of the world.

A leading multinational industry coalition that focuses on phishing, the Anti-Phishing Working Group (APWG), issues regular reports about the current volume and types of phishing attacks. The APWG's most recent statistics for August 2006 show the growth and variety of phishing attacks over the past year and more.[iii] In the month of August 2006, for example,

- The APWG received 26,150 unique phishing reports (compared to 13,776 in August 2005 and 6,957 in October 2004). This total represents the second highest number of phishing reports that the APWG has received in a single month.
- The APWG detected 10,091 unique phishing websites worldwide (compared to 5,259 websites detected in August 2005, and only 1,142 in October 2004[iv]).
- 148 separate corporate brands were "hijacked" (misused) in phishing schemes (compared to 84 in August 2005[v]).
- The financial sector was the most heavily targeted for phishing schemes, constituting 92.6 percent of all phishing attacks (compared to 84.5 percent in August 2005).[vi] (For example, leading financial institutions in Canada and the United States, as well as smaller U.S. financial institutions such as credit unions, have frequently been targeted.)
- The APWG found 2,303 unique websites that hosted "keylogging" programs—i.e., programs that record all keystrokes made at a particular computer, enabling criminals to obtain others' usernames, passwords, and other valuable data (compared to 958 such websites in August 2005 and 260 websites in April 2004[vii]). In comparison, the number of unique computer applications that included malicious code such as keylogging software has remained relatively constant (172 in August 2006, compared to 168 in August 2005).

- The United States was the country hosting the largest percentage of phishing websites (27.7 percent, compared to 27.9 percent in August 2005), while Canada ranked ninth among countries hosting such websites (2.2 percent, compared to 2.21 percent in August 2005). China remains the second most frequent host of phishing websites (14 percent, compared to 12.15 percent in August 2005), and South Korea the third most frequent host of such sites (9.59 percent, compared to 9.6 percent in August 2005[viii]).

Similarly, the Symantec Internet Security Threat Report[ix] for September 2006 reported that from January 1 to June 30, 2006, a total of 157,477 unique phishing messages were detected. This total represents an 81 percent increase over the 86,906 unique phishing messages detected in the preceding six months (July 30 – December 31, 2005) and a 612 percent increase over the 97,592 unique phishing messages detected in the first six months of 2005.[x] Finally, an AOL Canada study reportedly found that nearly one out of three Canadians surveyed had received an e-mail from a company seeking confirmation of their account information.[xi]

In general, phishing schemes have relied heavily on indiscriminate sending of "spam" e-mail to large numbers of Internet users, without regard to the demographic characteristics of those users. But some phishing schemes might disproportionately affect certain segments of the population.[xii] In addition, some phishing schemes, known colloquially as "spear phishing," seek to target more precisely defined groups of online users.[xiii] (See page 8 below.)

The short term effect of these scams is to defraud individuals and financial institutions. Some prior data suggest that in some phishing schemes, criminals were able to convince up to 5 percent of recipients to respond to their e-mails, resulting in a significant number of consumers who have suffered credit card fraud, identity fraud, and financial loss.[xiv] In the long run, phishing may also undermine public trust in the use of the Internet for online banking and e-commerce.

Although data on phishing attempts provide important indications of the dimensions of the phishing problem, several obstacles may prevent complete and accurate measurement. First, victims often have no idea how criminals obtained their data. Victims typically provide their personal information to phishers precisely because they believe the solicitation to be trustworthy. The unexplained and unexpected charges that later appear on their credit card statements often occur so long after the phishing solicitation, and involve items having no relation to the original subject matter of the phishing e-mails and websites, that victims have no reason to understand that there is a connection between these events.

Second, companies that are victimized by phishing may not report these instances to law enforcement. Unlike some other types of Internet-based crime**,** such as hacking**,** that may be conducted surreptitiously, phishing, by its nature, involves public misuse of legitimate companies' and agencies' names and logos. Nonetheless, some companies may be reluctant to report all such instances of phishing to law enforcement -- in part because they are concerned that if the true volume of such phishing attacks were made known to the public, their customers or accountholders would mistrust the companies or they would be placed at a competitive disadvantage.

As these statistics indicate, phishing continues to be a rapidly growing form of online identity theft that can cause both short-term losses and long-term economic damage. In either event, phishing scams and other identity theft crimes create significant costs that may ultimately be borne by consumers in the form of increased fees from the credit card companies or higher prices from the merchants who accept credit cards.

How Is Phishing Committed?

In a typical phishing scheme, criminals who want to obtain personal data from people online first create unauthorized replicas of (or "spoof") a real website and e-mail, usually from a financial institution or another company that deals with financial information, such as an online merchant. The e-mail will be created in the style of e-mails by a legitimate company or agency, using its logos and slogans. The nature and format of the principal website creation language, Hypertext Markup Language, make it very easy to copy images or even an entire website. While this ease of website creation is one of the reasons that the Internet has grown so rapidly as a communications medium, it also permits the abuse of trademarks, tradenames, and other corporate identifiers upon which consumers have come to rely as mechanisms for authentication.

Phishers typically then send the "spoofed" e-mails to as many people as possible in an attempt to lure them in to the scheme. (In some "spear phishing" attacks (see section on "Spear Phishing" below), phishers have used other illegal means to obtain personal information about a group of people, then targeted that specific group with e-mails that include illegally obtained information to make the e-mails appear more plausible.) These e-mails redirect consumers to a spoofed website, appearing to be from that same business or entity. The criminals know that while not all recipients will have accounts or other existing relationships with these companies, some of them will and therefore are more likely to believe the e-mail and websites to be legitimate. The concept behind many phishing attacks is similar to that of "pretext" phone calls (i.e., phone calls from persons purporting to be with legitimate institutions or companies asking the call recipients for personal information). In fact, the criminals behind these e-mails, websites, and phone calls have no real connection with those businesses. Their sole purpose is to obtain the consumers' personal data to engage in various fraud schemes.[xv]

Phishing schemes typically rely on three elements. First, phishing solicitations often use familiar corporate trademarks and tradenames, as well as recognized government agency names and logos. The use of such trademarks is effective in many cases because they are familiar to many Internet users and are more likely to be trusted without closer scrutiny by the users. Moreover, the indicators that are provided for web browsers to assess the validity and security of a website (e.g., the lock icon or the address bar) can all be spoofed. This problem is further compounded by the lack of standardized protocols among financial institutions for how they will communicate with their customers and what information they will request via the Internet.

Second, the solicitations routinely contain warnings intended to cause the recipients immediate concern or worry about access to an existing financial account. Phishing scams typically create a sense of urgency by warning victims that their failure to comply with instructions will lead to account terminations, the assessment of penalties or fees, or other negative outcomes. The fear that such warnings create helps to further cloud

the ability of consumers to judge whether the messages are authentic. Even if a small percentage of people who receive these fraudulent warnings respond, the ease with which such solicitations can be distributed to millions of people creates a sizable pool of victims. (It should be noted that some schemes instead are based on offering positive incentives, for example by offering the promise of a payment in return for taking part in an online survey.)

Third, the solicitations rely on two facts pertaining to authentication of the e-mails: (1) online consumers often lack the tools and technical knowledge to authenticate messages from financial institutions and e-commerce companies; and (2) the available tools and techniques are inadequate for robust authentication or can be spoofed. Criminals can therefore use techniques, such as forging of e-mail headers and subject lines, to make the e-mails appear to come from trusted sources, knowing that many recipients will have no effective way to verify the true provenance of the e-mails.

Example – ***Phishing scam targets Royal Bank Customers***

In June 2004, the Royal Bank of Canada notified customers that fraudulent e-mails purporting to originate from the Royal Bank were being sent out asking customers to verify account numbers and personal identification numbers (PINs) through a link included in the e-mail. The fraudulent e-mail stated that if the receiver did not click on the link and key in his client card number and pass code, access to his account would be blocked. These e-mails were sent within a week of a computer malfunction that prevented customer accounts from being updated. The malfunction impacted payroll deposits that were scheduled to enter many accounts, leaving customers at risk of missing mortgage, rent and other payments. The Royal Bank believes it is likely someone tried to take advantage of the situation.

Variants of Phishing

In the first generation of phishing schemes, most phishing attacks relied on the combination of fraudulent e-mails with links to fraudulent websites to obtain Internet users' information. Over the past two years, criminals have increasingly refined their phishing attacks by incorporating various other techniques to contact prospective victims or obtain their information.

"Spear Phishing"

"Spear phishing" is a colloquial term that can be used to describe any highly targeted phishing attack. Spear phishers send spurious e-mails that appear genuine to a specifically identified group of Internet users, such as certain users of a particular product or service, online account holders, employees or members of a particular company, government agency, organization, group, or social networking website. Much like a standard phishing e-mail, the message appears to come from a trusted source, such as an employer or a colleague who would be likely to send an e-mail message to everyone or a select group in the company (e.g., the head of human resources or a computer systems administrator). Because it comes from a known and trusted source, the request for valuable data such as user names or passwords may appear more plausible.

Whereas traditional phishing scams are designed to steal information from individuals, some spear phishing scams may also incorporate other techniques, ranging from computer hacking to "pretexting" (the practice of getting personal information under false pretences), to obtain the additional personal information needed to target a particular group or to enhance the phishing e-mails' credibility. In essence, some criminals will use any information they can to personalize a phishing scam to as specific a group as possible.[xvi]

Example – *Phishing expedition at heart of AT&T hacking*

In a recent scam, AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers and credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers.[xvii]

Redirection and Other Malicious Code-Based Schemes

A second technique that phishers use is to cause targeted Internet users to unknowingly download certain forms of malicious computer code into their office or home computers. One type of phishing scheme that uses malicious code is the so-called "redirection" scheme. Ordinarily, when an Internet user types the address of a particular website (such as "http://reallymybank.com") into an Internet browser, the computer directs the user to the correct website. In a redirection scheme, the malicious code introduced by phishers changes the code inside a user's computer so that, when the user tries to access a particular site by tying in the correct address, the code causes the user, without his knowledge, to be redirected to a phishing website that closely resembles the site that the user intended to access.

Another type of malicious code-related phishing scheme involves the use of keylogging software or a "backdoor" (i.e., code that allows criminals to access a user's computer without the user's knowledge). Once the phisher has caused an Internet user unknowingly to download malicious code that includes the keylogging software to his computer, the keylogger is typically set to operate only when the Internet user uses an Internet browser to access an online financial account. By recoding the user's keystrokes during the log-in process, then retrieving the keystroke data, the phisher can later use the keystroked data to reproduce the user's username and password and access the user's account to make substantial withdrawals from that account. The phisher may even use a "backdoor" to conduct the transaction directly from the user's own computer. This latter technique is intended to deceive security personnel at the financial institution where the user has his account. The user who reports that his account has been illegally accessed is less likely to be believed at first when the financial institution's security personnel trace the unauthorized transaction back to that user's computer.

"Vishing"

A phishing technique that has received substantial publicity of late is "vishing," or voice phishing. Vishing can work in two different ways. In one version of the scam, the consumer receives an e-mail designed in the same way as a phishing e-mail, usually indicating that there is a problem with the account. Instead of providing a fraudulent link to click on, the e-mail provides a customer service number that the client must call and is then prompted to "log in" using account numbers and passwords. The other version of the scam is to call consumers directly and tell them that they must call the fraudulent customer service number immediately in order to protect their account. Vishing criminals may also even establish a false sense of security in the consumer by "confirming" personal information that they have on file, such as a full name, address or credit card number.[xviii]

Vishing poses a particular problem for two reasons. First, criminals can take advantage of cheap, anonymous Internet calling available by using Voice over Internet Protocol (VoIP), which also allows the criminal to use simple software programs to set up a professional sounding automated customer service line, such as the ones used in most large firms. Second, unlike many phishing attacks, where the legitimate organization would not use e-mail to request personal information from accountholders, vishing actually emulates a typical bank protocol in which banks encourage clients to call and authenticate information.[xix]

Although banks will legitimately phone a client and ask questions to verify the client's identity, consumers must remember that a bank will never ask for PINs or passwords. It is also important that consumers never trust a phone number provided in an e-mail, and instead contact the institution through a number that has been independently verified or obtained through directory assistance. As noted above, this might include the telephone number or website printed on the back of their credit cards or on monthly account statements.

Consumers, law enforcement, and the private sector should assume that as public education about phishing increases, criminals will continue to use these variants but also develop additional variants and refinements to phishing techniques.

The Impact of Phishing

Phishing has four distinct types of impact, both domestically and internationally, that are of concern to the commercial and financial sectors and to law enforcement in both countries:

- *Direct Financial Loss*. Depending on the type of fraud that a criminal commits with the aid of stolen identifying data, consumers and businesses may lose anywhere from a few hundred dollars to tens of thousands of dollars. Indeed, small e-commerce businesses may be particularly hard-hit by identity fraud. For example, because of credit card association policies, an online merchant who accepts a credit card number that later proves to have been acquired by identity theft may be liable for the full amount of the fraudulent transactions involving that card number.

- *Erosion of Public Trust in the Internet*. Phishing also undermines the public's trust in the Internet. By making consumers uncertain about the integrity of commercial and financial websites, and even the Internet's addressing system, phishing can make them less likely to use the Internet for business transactions. People who cannot trust where they are on the World Wide Web are less likely to use it for legitimate commerce and communications.[xx]

  This perspective finds support in a 2005 *Consumer Reports* survey, which showed declining confidence in the security of the Internet. Among several findings, the survey found that 9 out of 10 American adult Internet users have made changes to their Internet habits because of the threat of identity theft, and of those, 30 percent say that they reduced their overall usage. Furthermore, 25 percent say they have stopped shopping online, while 29 percent of those that still shop online say they have decreased the frequency of their purchases.[xxi]

- *Difficulties in Law Enforcement Investigations*. Unlike certain other types of identity theft that law enforcement agencies can successfully investigate in a single geographic area (e.g., theft of wallets, purses, or mail), phishing – like other types of crime that exploit the Internet -- can be conducted from any location where phishers can obtain Internet access. This can include situations in which a phisher in one country takes control of a computer in another country, then uses that computer to host his phishing website or send his phishing e-mails to residents of still other countries. Moreover, online criminal activity in recent years has often reflected clearcut divisions of labor. For example, in an online fraud scheme, the tasks of writing code, locating hosts for phishing sites, spamming, and other components of a full-scale phishing operation may be divided among people in various locations. This means that in some phishing investigations, timely cooperation between law enforcement agencies in multiple countries may be necessary for tracing, identification, and apprehension of the criminals behind the scheme.

- *Incentives for Cross-Border Operations by Criminal Organizations*. Law enforcement authorities in Canada and the United States are concerned that each of the preceding factors also creates incentives for members of full-fledged criminal organizations in various countries to conduct phishing schemes on a systematic basis. Law enforcement already has indications that criminal groups in Europe are hiring or contracting with hackers to produce phishing e-mails and websites and develop malicious code for use in phishing attacks.

A Prevention and Reporting Checklist for Phishing Schemes

One of the most basic measures that government and the private sector are taking to protect the public from phishing is the provision of specific advice to the public about how to avoid phishing schemes and how to report phishing schemes. It is important to note that, according to a recent phishing study by researchers at Harvard University and the University of California at Berkeley, good phishing websites fooled 90 percent of the participants, nearly one-quarter of the participants did not look at existing anti-phishing

visual cues (e.g., security indicators), and "some visual deception [phishing] attacks can fool even the most sophisticated users."[xxii]

The following list of advice to the public—derived from information provided by the APWG, the U.S. Federal Trade Commission, and PhoneBusters (the National Call Centre in Canada)[xxiii]—is divided into four parts:

1. **Prevention: What to Do**

- Protect your computer with anti-virus software, spyware filters, e-mail filters, and firewall programs, and make sure that they are regularly updated.
    - Consider installing a Web browser tool bar to help protect you from known phishing fraud websites. (Check with your browser or e-mail provider for such toolbars.)

- Ensure that your Internet browser is up to date and security patches applied.
    - In particular, people who use the Microsoft Internet Explorer browser should immediately go to the Microsoft Security home page—http://www.microsoft.com/security/—to download a special patch relating to certain phishing schemes.

- Be suspicious of any e-mail with urgent requests for personal financial information or threats of termination of online accounts.
    - Unless the e-mail is digitally signed, you can't be sure it wasn't forged or "spoofed."
    - Phishers typically ask for information such as usernames, passwords, credit card numbers, social security numbers, etc.
    - Phisher e-mails are typically not personalized, while valid messages from your bank or e-commerce company generally are.

- When contacting your financial institution, use only channels that you know from independent sources are reliable (e.g., information on your bank card, hard-copy correspondence, or monthly account statement), and don't rely on links contained in e-mails, even if the web address appears to be correct.

- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser.
    - To make sure you're on a secure Web server, check the beginning of the Web address in your browsers address bar - it should be "https://" rather than just "http://."

- Regularly log into your online accounts.
    - Don't leave them for as long as a month before you check each account.

- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate.
    - If anything is suspicious, contact your bank and all card issuers.

2. Prevention: What Not to Do

- Don't assume that you can correctly identify a website as legitimate just by looking at its general appearance.

- Don't use the links in an e-mail to get to any web page, if you suspect the message might not be authentic.
    - Instead, call the company on the telephone, or log onto the website directly by typing in the Web address in your browser.

- Avoid filling out forms in e-mail messages or pop-up windows that ask for personal financial information.
    - You should only communicate information such as credit card numbers or account information via a secure website or the telephone.

3. Reporting: Suspicious E-mails and Websites

- Always report a "phishing" or "spoofed" e-mail or website to the following groups, whether or not you responded to that phishing e-mail or website:
    - Forward the e-mail to reportphishing@antiphishing.com
    - Forward the e-mail to the "abuse" e-mail address at the company that is being spoofed (e.g. "spoof@ebay.com")
    - In the United States, forward the e-mail to the Federal Trade Commission (FTC) at spam@uce.gov and notify the Internet Crime Complaint Center (IC3) by filing a complaint on its website, http://www.ifccfbi.gov.
        - The IC3 is a joint venture of the FBI and a non-profit organization, the National White Collar Crime Center (NW3C). Through the IC3 website, victims of online crime, including identity theft, can report possible criminal activity. Staff at IC3 analyze these complaints for patterns and levels of possible criminal conduct and, in appropriate cases, provide investigative packages of complaint data and other information to federal, state or local investigators and prosecutors in various metropolitan areas throughout the U.S. The IC3 also shares its Internet fraud and identity theft complaint data with the FTC for inclusion in the FTC's Identity Theft Data Clearinghouse.
        - The FTC developed the Data Clearinghouse in late 1999, to establish a central nationwide repository for law enforcement access to identity theft complaints. Built on the FTC's Consumer Sentinel network, the Clearinghouse provides both U.S. and Canadian members of the Sentinel network with direct, online and secure access to the consumer complaints that the FTC receives through its online complaint form at http://www.consumer.gov/idtheft, a toll-free hotline (1 877 IDTHEFT) and data sharing agreements with other entities, including the Social Security Administration's Office of the Inspector General. Law enforcement officers can search the Clearinghouse database for complaints based on the location of a suspect, a victim or a particular company involved in the misuse of the identities, or many other key elements of the crime. Currently

more than 1,000 law enforcement agencies have direct online access to almost 700,000 identity theft complaints through the Clearinghouse.

- Note: When forwarding spoofed messages, always include the entire original e-mail with its original header information intact.

4. Reporting: Possible Disclosures to Phishers

- If you believe that you have disclosed information in response to a phishing scheme, notify law enforcement authorities immediately.
  - In the United States, notify the Internet Crime Complaint Center (IC3) by filing a complaint on its website, http://www.ifccfbi.gov.
  - In Canada, notify the Royal Canadian Mounted Police by filing a complaint on the Reporting Economic Crime Online (RECOL) website at http://www.recol.ca/, and obtain information about how to deal with identity theft by contacting the PhoneBusters National Call Centre at http://www.phonebusters.com/.
    - RECOL is a web-based initiative that involves an integrated partnership between international, federal and provincial law enforcement agencies, as well as regulators and private commercial organizations that have a legitimate investigative interest in receiving a copy of complaints of economic crime, including identity theft. RECOL also provides data pertaining to trends, as well as information relating to consumer education, prevention and awareness of economic crime.)
    - The PhoneBusters National Call Centre (PhoneBusters) is the Canadian anti-fraud call centre, jointly operated by the Ontario Provincial Police (OPP) and the Royal Canadian Mounted Police (RCMP), that collects information on telemarketing fraud, advanced fee fraud letters and identity theft complaints. Although it has e-mail capacity, most complaints are phoned in to PhoneBusters. The information is then disseminated to the appropriate law enforcement agencies. Due to the ever-increasing number of complaints about identity theft, PhoneBusters started an Identity Theft project in 2002. The data collected at PhoneBusters is a valuable tool in evaluating the effects on the public of various types of fraud. PhoneBusters plays a key role in educating the public about specific fraudulent telemarketing pitches, and also plays a vital role in the collection and dissemination of victim evidence, statistics and documentation. The original mandate of PhoneBusters was to prosecute key individuals in Ontario and Quebec involved in telemarketing fraud under the *Criminal Code of Canada*, but this has been expanded to include facilitating prosecution by U.S. agencies through extradition, and by Industry Canada under the *Competition Act*. In the fall of 2006 PhoneBusters will begin to collect statistics and information relating directly to phishing through the merged Internet reporting opportunities with RECOL.

- Note: A wide range of federally regulated financial institutions in the United States is required to file Suspicious Activity Reports (SARs) with the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN),

whenever they encounter information that indicates a crime affecting a financial institution (including phishing) may have been committed. U.S. law enforcement agencies may access these reports for investigative purposes. More recently, in response to the growing incidence of identity theft, these reports, known as Suspicious Activity Reports, have been revised to include a box that a financial institution may check if it believes that identity theft is involved in some way with the suspicious activity it is reporting. This revision increases the opportunities for federal agents to identify current or recent identity theft-related crimes affecting financial institutions.

Responses to Phishing: Current and Promising Practices

Private-sector entities and government agencies in Canada and the United States have undertaken a growing variety of measures and initiatives to combat phishing. As explained below, many of these measures and initiatives are multi-sectoral, multi-jurisdictional, and multi-agency, and extend beyond law enforcement entities.

Public Education

Because phishing is a form of identity theft that differs substantially from other, physically-based identity theft techniques, government and the private sector need to ensure that the public receives regularly updated information about the latest phishing techniques and how to recognize them. At the May 2003 Cross-Border Crime Forum, PSEPC (then the Department of the Solicitor General of Canada) and the U.S. Department of Justice jointly issued two public advisories on current trends and developments in identity theft: one directed at consumers and the other at retailers. The advisories highlighted some of the most significant forms of identity theft in Canada and the United States, explaining how to recognize them and how to respond. Since then, various Canadian and U.S. law enforcement agencies have widely disseminated phishing-related information to the public. For example, the U.S. Department of Justice issued a special public advisory on phishing in 2004,[xxiv] the U.S. FTC issued a consumer alert on phishing in 2005,[xxv] and the RCMP has recently posted information about phishing and vishing on its website.[xxvi]

Authentication

Although consumer education programs are an important component of the fight against phishing and other forms of identity theft that involve “social engineering,” they will not suffice to provide adequate protection for the public as phishers continue to refine their attack techniques. The private sector needs to continue its efforts to improve authentication technologies, and to deploy multifactor authentication measures as appropriate, to strengthen the confidence of Internet users in the reliability and provenance of online messages they receive. Greater industry efforts towards standardizing how enterprises will communicate with their clients (e.g., what information they will use for authentication purposes and under what circumstances they will request it) may also be important in addressing this issue.

Legislative Frameworks

A strong legislative framework is also fundamental to combating identity theft, and specific mechanisms and/or methods used to that end such as phishing. In Canada, there are currently no offences in the *Criminal Code* that directly prohibit or apply to phishing or other methods of obtaining identity information for a criminal purpose. If a phishing attack is using large volumes of "spam" (unsolicited e-mails) that could interfere with a computer system, or if the spam employs deceptive headers so as to avoid spam filters, then certain computer data related offences in the *Criminal Code* may apply. The use of identity information that has been obtained whether by phishing or by other means, could however amount to any of a number of criminal offences, such as fraudulent personation, fraud, or unlawful use of credit card data. The Department of Justice began several years ago to review the *Criminal Code* to determine its adequacy for dealing with the growing problem of identity theft. The Department has begun developing proposals to address some of the limitations of the criminal law in this area and consulting with key stakeholders to obtain their valuable input on legislative amendments.

Another recent development in Canada with implications for phishing-related legislation was the 2004 launch by the Government of Canada of *An Anti-Spam Action Plan for Canada* and the establishment of a government-private sector task force to oversee and coordinate its implementation. In 2005 this task force was asked to produce a report on the status and progress that had been made. The report that they produced, *Stopping Spam: Creating a Stronger, Safer Internet*, set forward 22 recommendations to combat spam, promote public awareness, and restore confidence in e-mail. They also set forward best practices for Internet service providers and other network operators, and for e-mail marketing. Additionally, they recommend that legislation be enacted to prohibit certain forms of spam and other emerging threats to the safety and security of the Internet (e.g. phishing), and that a federal coordinating body should be established to deal with the spam issue on an ongoing basis.[xxvii] This is important for the phishing issue because phishing is usually accomplished through the technique of spamming, which is the sending out of unsolicited bulk e-mails. In the case of phishing, spam routinely allows criminals to distribute their fraudulent e-mails to many consumers at minimal cost.

In the United States, since 1998 federal law, and laws in nearly all of the states, have adopted specific criminal legislation on identity theft that can be applied to phishing.[xxviii] In addition, federal authorities can use a variety of federal fraud offences, such as wire fraud,[xxix] and the CAN-SPAM Act,[xxx] to address both the sending of phishing e-mails and the use of deceptive e-mail headers or other techniques characteristic of criminal spam. Currently, at the direction of President Bush, the President's Identity Theft Task Force is preparing a strategic plan to combat all forms of identity theft more effectively, including possible changes in legislation where appropriate. That plan is expected to be submitted to the White House in early February 2007.[xxxi]

Enforcement

An effective and comprehensive response to identity theft requires the investigation and prosecution of appropriate cases involving phishing schemes. Within the last year, the

United States has brought a number of federal criminal prosecutions of phishers. For example:

- In August 2006, a Florida man was indicted by a U.S. federal grand jury on charges of wire fraud related to a phishing scheme that included among its targets people seeking to donate to Hurricane Katrina disaster relief efforts. The defendant allegedly created and sold fraudulent "phishing" web sites. The phishing web sites, packaged in "phishing kits" that sometimes included online testimonials requesting donations, deceived visitors into believing they were providing their personal and financial information to a legitimate web site. Among the fraudulent web sites that the defendant allegedly created were ones mimicking sites for the American Red Cross Hurricane Katrina disaster relief efforts and two Canadian financial institutions, Banque Nationale and Desjardins Credit Union. He allegedly sold the phishing sites to would-be scammers for approximately $150 each. One such site, for Banque Nationale, received approximately 8,500 "hits."[xxxii]

- In May 2006, an Iowa man was sentenced to 21 months imprisonment for operating a phishing scam targeting MSN customers. The defendant was convicted after pleading guilty to wire fraud and fraud and related activity in connection with access devices. The sentence also included an order that the defendant pay restitution in the amount of $57,294.07. The defendant admitted that he created a bogus MSN (a division of Microsoft Corporation) website, then sent e-mails to MSN customers requesting that they visit the website and update their accounts by providing credit card account numbers and other personal information. Harris deceived MSN customers into believing that this would result in a fifty percent credit towards their next monthly bill. When the recipients submitted information, it was sent to an e-mail address that Microsoft was eventually able to trace back to the defendant's address in Davenport.[xxxiii]

- In January 2006, a California man was arrested on charges of wire fraud and the unauthorized use of an access device (credit card) in connection with a phishing scam targeting AOL customers. The defendant is accused of sending thousands of e-mails to America Online (AOL) users that appeared to be from AOL's Billing Department. Those fraudulent messages urged the subscribers to "update" their AOL billing information or lose service, and referred them to one of several fraudulent Internet websites where they could input personal and financial account information. The defendant, who allegedly controlled those websites, used the fraudulently obtained information to make unauthorized charges on the credit or debit cards belonging to the duped AOL subscribers. This case was investigated by U.S. authorities with substantial assistance from the Ontario, California Police Department.

Effective investigation and prosecution of phishing, however, also requires that law enforcement authorities (including investigators and prosecutors) receive training on phishing schemes and investigative techniques as part of their training on identity theft. In Canada, the Ontario Provincial Police has organized three international conferences on identity theft that have drawn hundreds of investigators from across Canada, the United States, and other countries. In the United States, the Department of Justice, through its National Advocacy Center, conducts training on phishing and other forms of

identity theft for federal agents and prosecutors. In addition, both the Canadian Association of Chiefs of Police and the International Association of Chiefs of Police have components that focus specifically on identity theft and cybercrime issues.

Binational and National Coordination

Identity theft-related issues, including phishing, cut across all jurisdictions and involve all levels of government, the law enforcement community, and the private sector. In an effort to avoid duplication of activities and to ensure consistency across all jurisdictions and programs, a number of coordinating bodies has been established at the national, binational, and multinational levels that have been addressing different aspects of identity theft. Because of their interest in and mandate over identity theft, these bodies are also well-suited to facilitate binational and national coordination on phishing in particular.

- **Binational Working Group on Cross-Border Mass Marketing Fraud / Cross-Border Crime Forum** –Since 1997, the Binational Working Group on Cross-Border Mass Marketing Fraud has provided an important mechanism for binational coordination and cooperation on a wide variety of mass marketing fraud issues. This Working Group, which also functions as a sub-group of the Canada-U.S. Cross-Border Crime Forum, has previously highlighted the problem of identity theft through its 2003 report on mass-marketing fraud and its involvement in the preparation of joint public advisories on identity theft for distribution in both countries. Once the strategic plan of the President's Identity Theft Task Force is publicly announced, the Binational Working Group may provide one of the mechanisms for specific discussions about binational coordination of public education, prevention, and enforcement relating to phishing and other forms of identity theft.

- **United Nations Crime Commission Intergovernmental Expert Group on Fraud and the Criminal Misuse of Identity**. Since 2005, under the direction of the United Nations Crime Commission, an Intergovernmental Expert Group has been studying the related problems of fraud and the criminal misuse of identity. The Expert Group, in which both Canada and the United States are active participants, is now preparing a report to the Crime Commission that is expected to include specific discussions of online identity theft, including phishing, as well as recommendations for best practices by government and the private sector.

Conclusion

Phishing is a form of criminal conduct that poses increasing threats to consumers, financial institutions, and commercial enterprises in Canada, the United States, and other countries. Because phishing shows no sign of abating, and indeed is likely to continue in newer and more sophisticated forms, law enforcement, other government agencies, and the private sector in both countries will need to cooperate more closely than ever in their efforts to combat phishing, through improved public education, prevention, authentication, and binational and national enforcement efforts.

While phishing is a particular threat on its own, it is also important to recognize that the challenges posed to policy makers and law enforcement officials in regards to phishing are those reflected in the larger issue of identity theft as well.

The Report on identity theft presented to the Binational Working Group on Cross-Border Mass Marketing Fraud in October 2004 sets out recommendations to address the threats posed by identity theft, including coordinating public education initiatives, enhancing reporting mechanisms and enforcement, reviewing legislative frameworks and improving document and data integrity and security.[xxxiv]

This report further endorses those recommendations in support of the fight against phishing and identity theft as a whole. In response to those recommendations governments in both countries will continue to work together in an effort to reduce phishing and identity theft.

[i] Report on Identity Theft, October 2004, available at http://www.psepc-sppcc.gc.ca/prg/le/bs/report-en.asp.
[ii] Phishing: A new form of identity theft – A Joint Canada/US Public Advisory, - *Cross Border Crime Forum*, October 2004 – http://www.psepc.gc.ca
[iii] Anti-Phishing Working Group, Phishing Activity Trends Report: August, 2006, *available at* http://www.antiphishing.org/reports/apwg_report_August_2006.pdf.
[iv] Anti-Phishing Working Group, Phishing Activity Trends Report: August, 2005, *available at* http://www.antiphishing.org/reports/apwg_phishing_activity_report_august_05.pdf.
[v] APWG, August 2005
[vi] APWG, August 2005
[vii] APWG, August 2005
[viii] APWG, August 2005
[ix] Symantec is an international corporation that provides software, appliances, and services to help customers assure the security, availability, and integrity of their information assets and infrastructure. The Symantec Internet Security Threat Report offers analysis and discussion of threat activity over a six-month period. It covers Internet attacks, vulnerabilities, malicious code, phishing, spam, security risks, and future trends.
[x] Symantec Corporation, Internet Security Threat Report at 22 (September 2006), *available at* http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf.
[xi] See Dan Ferguson, Black Press, *Phishing warning Beware e-mails asking for personal info*, Peace Arch News, October 10, 2006, *available at* http://www.peacearchnews.com/portals-code/list.cgi?paper=44&cat=23&id=746625&more=.
[xii] Internet Scams Fraud Trends: January-December 2005, *National Consumers League, available at* http://www.fraud.org/internet/intstat.htm.
[xiii] *See* Larry Greenemeier, Update: AT&T Hackers Devised Elaborate Phishing Scam To Dupe Customers, Information Week, September 1, 2006, *available at* http://informationweek.com/news/showArticle.jhtml?articleID=192501168.
[xiv] Phishing Activity Trends Report- January 2005, *The Anti-Phishing Working Group.*
[xv] Pretexting is not done solely to further phishing or other forms of online identity theft and fraud. As recent news reports indicate, pretexting may also be done for other unethical or illegal purposes.
[xvi] Spear Phishing: Highly Targeted Scams, *Microsoft*, December 9, 2005. www.microsoft.com
[xvii] Lazarus, David. Phishing expedition at heart of AT&T hacking, San Francisco Chronicle, September 1, 2006. www.sfgate.com
[xviii] FCAC Cautions Consumers About New "Vishing" Scam, *Financial Consumer Agency of Canada*, July 25, 2006.
[xix] Schulman, Jay. Voice-over-IP Scams Set to Grow, *VoIP News*, July 21, 2006.
[xx] Stevenson, Robert Louis B. Plugging the "Phishing" Hole: Legislation Versus Technology, 2005 Duke Law and Technology Review 0006.
[xxi] Leap of Faith: Using the Internet Despite the Dangers, *Consumer Reports WebWatch*, October 2005. www.consumerwebwatch.org
[xxii] *See* Rachna Dhamija, J.D. Tygar, and Why Phishing Works paper presented at CHI 2006, April 22-27, 2006, Montréal, Quebec, *available at* http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf.
[xxiii] See Anti-Phishing Working Group, Consumer Advice: How to Avoid Phishing Scams, available at http://www.antiphishing.org/consumer_recs.html; PhoneBusters, Recognize It: Phishing, *available at* http://www.phonebusters.com/english/recognizeit_phishingemails.html.
[xxiv] See Criminal Division, U.S. Department of Justice, Special Report on "Phishing" (2004), available at http://www.usdoj.gov/criminal/fraud/Phishing.pdf.
[xxv] See FTC, Consumer Alert: How Not to Get Hooked by a ' Phishing' Scam, available at http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm.
[xxvi] See RCMP, Hameçonnage, « phishing » ou usurpation de marquee, *available at* http://www.rcmp-grc.gc.ca/scams/phishing_f.htm; RCMP,Vishing or Voice Phishing, available at http://www.rcmp-grc.gc.ca/scams/vishing_e.htm.
[xxvii] Stopping Spam: Creating a Stronger, Safer Internet, *Report of the Task Force on Spam,* May 2005

[xxviii] See 18 U.S.C. 1928(a)(&), 1028A(a).
[xxix] See 18 U.S.C. 1343.
[xxx] See 18 U.S.C. 1037.
[xxxi] *See* Executive Order (May 10, 2006), *available at* http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html.
[xxxii] See U.S. Attorney's Office, Western District of Pennsylvania, Press Release (August 16, 2006), available at http://www.usdoj.gov/katrina/Katrina_Fraud/pr/press_releases/2006/aug/08-16-06desirindict.pdf.
[xxxiii] See U.S. Attorney's Office, Southern District of Iowa, Press Release (May 19, 2006), available at http://www.usdoj.gov/usao/ias/press_releases/051906a.html.
[xxxiv] Report on Identity Theft, October 2004

Appendix 1: Bibliography

Consumer Advice: How to Avoid Phishing Scams. Anti-Phishing Working Group, *available at* http://www.antiphishing.org/consumer_recs.html.

Consumer Alert: How Not to Get Hooked by a "Phishing" Scam. FTC. June 2005, *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm.

Executive Order (May 10, 2006), *available at* http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html.

FCAC Cautions Consumers About New "Vishing" Scam, *Financial Consumer Agency of Canada*, July 25, 2006.

Ferguson, Dan. Black Press. Phishing warning Beware e-mails asking for personal info, Peace Arch News, October 10, 2006, *available at* http://www.peacearchnews.com/portals-code/list.cgi?paper=44&cat=23&id=746625&more=.

Hameçonnage, « phishing » ou usurpation de marquée. RCMP, a*vailable at* http://www.rcmp-grc.gc.ca/scams/phishing_f.htm

Internet Scams Fraud Trends: January-December 2005, *National Consumers League*, *available at* http://www.fraud.org/internet/intstat.htm.

Internet Security Threat Report: September 2006. *Symantec Corporation*.

Lazarus, David. Phishing expedition at heart of AT&T hacking, *San Francisco Chronicle*, September 1, 2006. www.sfgate.com

Leap of Faith: Using the Internet Despite the Dangers, *Consumer Reports WebWatch*, October 2005. www.consumerwebwatch.org

March Declared "Fraud Prevention Month" in Canada and Around the World, *Competition Bureau*, March 1, 2006, www.competitionbureau.gc.ca

Phishing: A new form of identity theft – A Joint Canada/US Public Advisory, - *Cross Border Crime Forum*, October 2004 – http://www.psepc.gc.ca

Phishing Activity Trends Report- January 2005. *The Anti-Phishing Working Group.* http://antiphishing.org

Phishing Activity Trends Report: August 2005. *The Anti-Phishing Working Group*.

Phishing Activity Trends Report- May 2006. *The Anti-Phishing Working Group*.

Phishing Activity Trends Report: August, 2006. *The Anti-Phishing Working Group*.

Recognize It: Phishing – *PhoneBusters*, www.phonebusters.com

Report on Identity Theft, October 2004

Schulman, Jay. Voice-over-IP Scams Set to Grow, *VoIP News*, July 21, 2006.

Spear Phishing: Highly Targeted Scams, *Microsoft*, December 9, 2005. www.microsoft.com

Special Report on "Phishing". Criminal Division, U.S. Department of Justice (2004), *available at* http://www.usdoj.gov/criminal/fraud/Phishing.pdf.

Statistics on Phone Fraud: Identity Theft Complaints (2005) – *PhoneBusters,* http://www.phonebusters.com/english/statistics_E05.html

Stevenson, Robert Louis B. Plugging the "Phishing" Hole: Legislation Versus Technology, 2005 Duke Law and Technology Review 0006.

Stopping Spam: Creating a Stronger, Safer Internet, *Report of the Task Force on Spam,* May 2005

Vishing or Voice Phishing, RCMP, *available at* http://www.rcmp-grc.gc.ca/scams/vishing_e.htm.