

Exposing Email-Borne Fraud

Volume 2 - Scam Prevention Guide

How to recognize a phish when you see one

Table of contents

Preface

Contributing experts
Introduction

Phishing 101

How phishing works
Targets and Victims

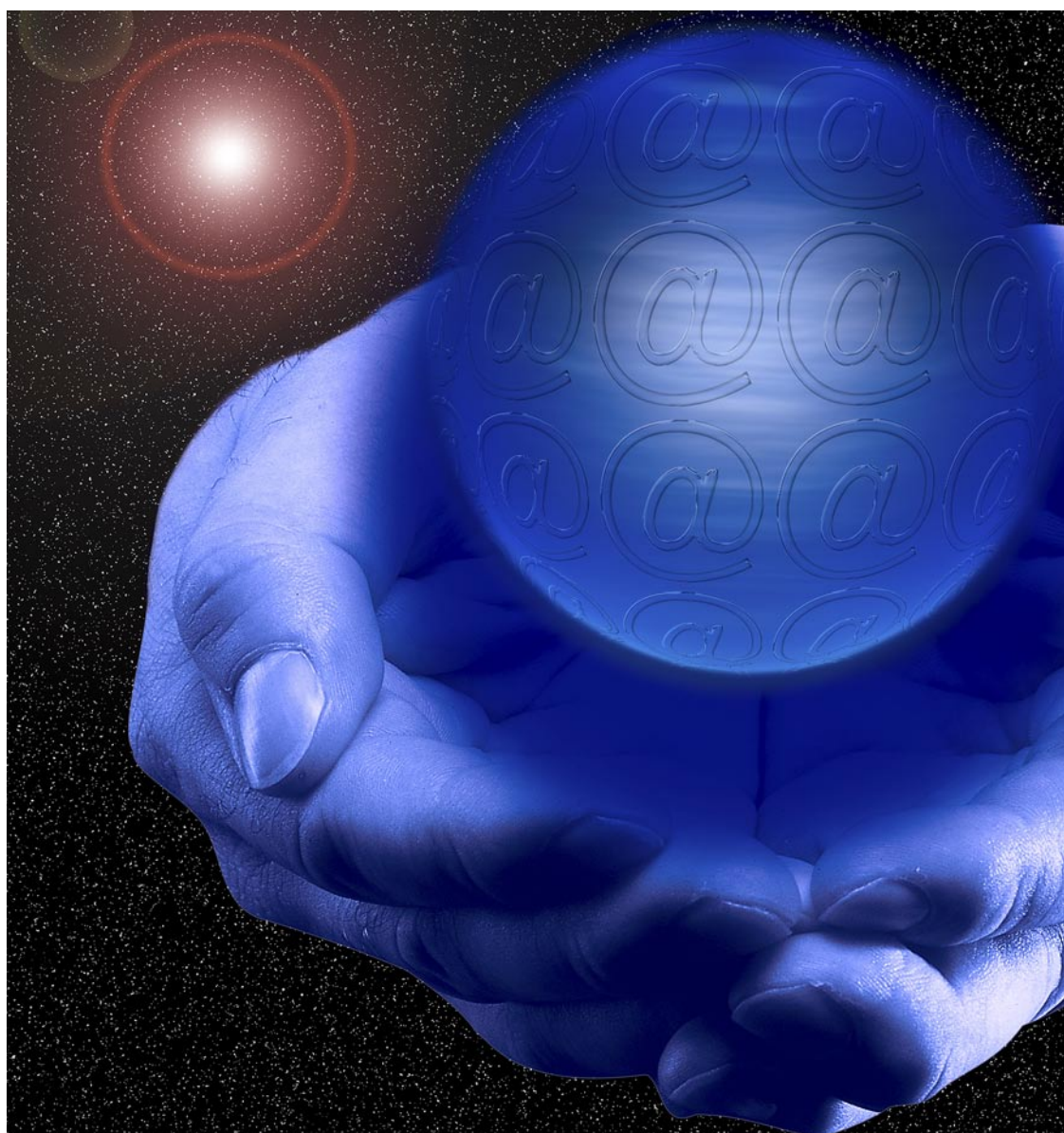
Phishing Tactics

Social Engineering
Address Spoofing
Brand Spoofing
Fake URLs
Timeliness
Call to action

Analysis of a Phishing Email

Recognize and Avoid Phishing Scams

A Final Note on Phishing



Norman is one of the world's leading companies within the field of data security. With products for virus control, spam control, email control, download control and personal firewall, the company plays an important role in the data industry.



NORMAN[®]
www.norman.com

Preface

The goal of this paper is not solely to explain phishing; it is also intended to emphasize how deceitful and dangerous phishing is. Today's technology facilitates the creation and dissemination of convincing, undetectable phishing emails. Consequently, it is alarmingly easy to fall victim to a phishing scam, irrespective of a person's familiarity with email technology.

While it may be extreme to suggest that users delete every unsolicited email they receive without reading it, Norman strongly urges email users to ignore requests for either personal or confidential information in unsolicited emails. The unfortunate reality today is that technology alone cannot stop phishing attacks. The surest way to avoid a phishing scam is to NEVER authenticate yourself in an unsolicited email by providing confidential information.

Contributing Experts

Vircom is one of Normans technology partner. The following Vircom contributors are quoted throughout this document, imparting extensive industry knowledge, messaging security expertise and important advice to readers.

Michael Gaudette

Michael is Vircom's director of product strategy. With a background in Internet infrastructure management, Michael leads Vircom's product development efforts and is responsible for maintaining synergy between Vircom's solutions and their respective markets.

Marc Chouinard

As head of the SpamBuster Team, Marc oversees Vircom's Internet spam monitoring efforts. Constantly developing preemptive tools that analyze spam patterns instead of instances, Marc ensures that the technology driving Vircom's Sequential Content Analyzer™ engine remains ahead of the latest spam tactics.

Introduction

What's in the average user's inbox? Newsletter from favorite trade e-zine? Check. Reminder about upcoming meeting? Check. Confirmation from online purchase? Check. Theft attempt of confidential information? Check. Check? That's right. Chances are, nestled among your legitimate emails is, has been or will be an unsolicited message designed to deceive and defraud: a phishing scam.

Phishing has become a popular form of email fraud that is more menacing than most spam - it is designed to defraud individuals and enterprises who, in turn, suffer financial loss, bad credit and tainted reputations.

Phishing is an aggressive form of fraud. Scammers who phish do not use a catch-and-release technique: when these fraudsters reel in victims, they take them hook, line and sinker.

Phishing 101

So what is phishing, exactly? What it boils down to is stealing. It's the act of deviously obtaining information and using it - without permission - for financial or other gain.

Unlike most spammers who try to get your money through persuasion, phishers unscrupulously steal it by posing as legitimate, reputable institutions and enterprises and using false pretenses to get victims to divulge confidential information.

How Phishing Works

Phishing attempts begin with an unsolicited email, purportedly from a legitimate enterprise or institution. Phishers bulk-send these emails, deliberately copying the look and tone of legitimate websites to establish credibility and gain the trust of unsuspecting recipients. This underhanded tactic, known as reputation hijacking, is used to steal confidential information and can end up costing victims their savings and enterprises their hard-earned reputations.

The key to a successful phishing attempt is to get recipients to click on a link in the phony email that takes them to a fake website. Once there, individuals are asked to authenticate themselves by providing confidential information such as passwords, bank account information, credit card numbers and social security numbers. In doing so, victims provide phishers with the tools they need to usurp identities and financial resources.

Phishing scams can generate between \$100,000 and \$200,000 per attack



Targets and Victims

Think you could never fall for a phishing scam? Consider this: at the 2004 Email Authentication Summit in Washington, D.C., it was reported that 33 percent of people who receive phishing scams click on links provided in the emails!

Many email users have a false sense of security about online privacy. But the reality is that anyone with an email address and a bank account, credit card, social security number or other confidential information is a potential victim of phishing.

To ensure the greatest profitability, phishers often target customers of high-profile companies. According to Vircom's SpamBuster team, more than 78 percent of targeted industries are in the financial or securities sector, while 19 percent of targets are online retailers such as eBay and Amazon. This strategy pays off nicely. As reported by a panel of industry experts at the 2004 Email Authentication Summit, phishing scams generate between \$100,000 and \$200,000 per attack.

"Citibank, eBay and PayPal are favourite phishing targets because they have millions of customers worldwide. The odds of a phishing scam reaching the mailbox of an eBay customer - and being opened - are much greater than if the scam spoofed a smaller, lesser known enterprise."

Phishing Tactics

Like scammers, phishers use distinctive techniques to con victims out of personal details, secure information and financial resources. Phishing emails characteristically include social engineering techniques, calls to action and forged URLs. Understanding and identifying these common phishing tactics is the first line of defense in avoiding them.

Social Engineering

Human interaction techniques, known as social engineering, are effective ways to gain access to private information. Phishers disguise their emails as important correspondence from trustworthy companies and carefully word messages so as to establish credibility and create a sense of urgency to respond.

Not only are phishers skilled at conning victims into divulging secure information, but they are also adept at deducing such information based on personal details like phone numbers, names of dependants, licence plate numbers and birthdays.

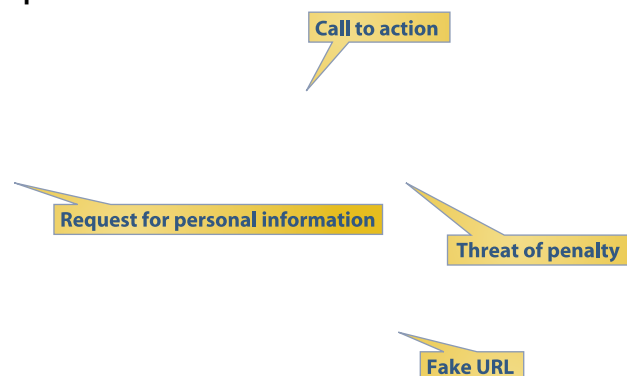
The Royal Bank of Canada (RBC) scam is a good example of social engineering. In August 2004, RBC experienced a temporary but widespread computer problem that left its customers in banking limbo for several days. Within 24 hours of this occurrence, phishers had taken advantage of the situation by bulk-emailing messages to Canadian addresses, pretending to be from the Royal Bank.

To safeguard their assets, many RBC customers followed the directives in the phony email and divulged account numbers, passwords and client card numbers - all of which phishers used to unlawfully acquire financial resources and assume clients' identities.

"While most scammers target the largest possible number of mailboxes, the RBC scammer(s) focused on mailboxes with addresses ending in .ca, which indicates a Canadian address. Because the Royal Bank is headquartered in Canada, concentrating on Canadian addresses was a good social engineering tactic to ensure a high number of victims."

The following is an excerpt from a fraudulent but convincing Royal Bank of Canada email sent to millions of Canadian inboxes during RBC's computer difficulties:

Example: Royal Bank Impersonation



Address Spoofing

Email address spoofing has created major problems for regulating Internet communications; it allows phishers to deceive victims, maintain anonymity and avoid detection and prosecution by authorities.

To conceal their real addresses, phishers use spoofed 'from' addresses (i.e. domain names belonging to others) to disseminate fraudulent emails. For example, a phisher could create a fraudulent email and send it to thousands of mailboxes using a forged address such as clientverification@trustedcompany.com. Unsuspecting recipients would be more likely to open the email if they believed it was sent by a trusted or legitimate sender.

Brand Spoofing

Replicated logos and graphics commonly associated with legitimate businesses and institutions are important tools that phishers use to deceive their victims. Phony websites are designed using copied logos, proprietary corporate colours and other professional-looking graphics... all of which lead to successful brand spoofing.

By using recognized colour schemes and high-quality logo reproductions, phishers can create fake websites that look almost identical to the legitimate, official websites of the targeted company or institution.

The Citizens Bank phishing attempt is a prime example of successful brand spoofing. In August 2004, Citizens Bank was the target of a phishing scam centered on a phony bill payment service.

Phishers spoofed the bank, creating a fake web page by replicating the bank's logo, corporate colours and other graphics. Although the visual quality of the spoofed site was not as good as that of the bank's official website, the difference was not enough to alert the average Citizens Bank customer.

"The web page set up for this scam was a true 'dummy' page. We tested it ourselves, entering several number combinations using anywhere from nine to sixteen numbers. We also tried using varied letter/number combinations; in each case, the combination we entered was accepted. Phishers with even the most basic knowledge of HTML coding can create copies of websites that look official. To the average person, these sites appear to be legitimate; so just imagine how hard it is to spot a fake website created by a proficient coder."

Fake URLs

By getting potential victims to click on a link that directs them to a phony website, phishers become one step closer to reaching their objective. Once on the phony website, victims are asked to supply confidential financial information - such as their bank account number and password or credit card information - in order to proceed.

If an email instructs you to visit a particular website or page by clicking on the link provided, don't. It's very easy to forge a link. As an example, the link in the Citizens Bank scam appeared as www.citizensbank.com/billpay/activate.asp; however, the link actually lead to <http://217.57.131.78/Citizens>, a site that was not associated with the bank.

Timeliness

Phishers are always on the lookout for opportunities to attack. Like any good predator, phishers seek out weaknesses they can exploit without rousing suspicion. Computer difficulties, corporate mergers and the implementation of new billing systems create perfect opportunities to initiate a phishing campaign.

That said, however, large financial institutions and well-known enterprises know they are perfect targets for phishers. Consequently, they take great care to implement technology and security measures that prevent scams and protect their clients from being victimized by phishers.

"While phishing attacks can occur at any time, phishers often time their mailings to coincide with computer or other technical difficulties experienced by reputable financial institutions. In the case of the Royal Bank of Canada, phishers launched their campaign one day after the bank began experiencing computer problems."

Important alert!

Never automatically click on a link! Even if a link looks official, it may not be. Are you being directed to a fraudulent website? Is someone trying to steal your confidential information?

Here's our advice:

- 1) Don't click on a link provided in any unsolicited email. Protect yourself by opening a new browser window then typing in the official web address of the enterprise or financial institution in question.
- 2) Once on the official homepage, look for information related to the subject of the email you received.
- 3) If you don't find the information you're looking for, delete the unsolicited email and contact the enterprise or institution using a number you know to be valid (i.e. the phone number appearing on a previous bill or other correspondence you received by mail).



Statistics

Unread email

Scan content

"A typical phishing scam can live for two or three days until it is discovered and the link is pulled. Some financial institutions have become so proficient at detecting phishing scams that it takes them half this time to inform authorities and post warnings to their customers."

Call to Action

Keywords and phrases create a sense of urgency and cause victims to react hastily. Phishers know that most email users are pressed for time and don't scrutinize every email for legitimacy, especially those that appear to have been sent by financial institutions.

In the following Citizens Bank and RBC examples, phishers made clients believe that failure to act would result in financial penalty or another undesirable consequence:

"Please fill in your card information now to avoid extra upgrade fees being withdrawn from your account later on." (Citizens Bank)

"This is required for us to continue to offer you a safe and risk free environment to send and receive money online." (RBC)

"Phishing scams targeting clients of financial institutions always include false or leading statements designed to scare victims into believing they will be subject to risk or penalty if they do not act immediately."

"Phishers want victims to react quickly because the longer the scam is circulating, the greater the chance of detection. People should always remember that no financial institution or reputable company will ask for secure or confidential information via email."

Important alert!

Spot the usual suspects

To avoid getting tangled up in a phishing scam, look for the following characteristics:

- Request for confidential information such as account numbers and passwords;
- Threat of penalty, cancellation, or other negative repercussion;
- Instruction to visit a web page by clicking on a link provided in the email;
- Sense of urgency or importance marked by request for immediate action.

No financial institution will ask for confidential information in an email.

Analysis of a Phishing Email: Citizens Bank Scam

In August 2004, Citizens Bank was the target of a phishing scam involving BillPay, a supposed online bill payment service available to the bank's client base. Vircom's SpamBuster team, which monitors thousands of emails per day, became aware of the phishing scam and alerted Citizens Bank immediately. The bank responded quickly, and within 12 hours of the discovery the phony web page was removed from the Internet. Citizens Bank also posted a warning on its website cautioning customers about the existence of online fraud and explaining common scams.

"The phisher(s) involved in the Citizens Bank scam asked potential victims for their ATM or MasterMoney Card Number, including the expiry date. Additionally, they requested people's Personal Identification Number (PIN). Under no circumstances should anyone give this type of information over the Internet. No bank or other financial institution would ever ask for this type of information in an email."

Several inconsistencies between the phishing email and the bank's official website indicated a scam; however, these were not obvious to the average Citizens Bank client and could have easily gone unnoticed. For example:

The resolution of the logo in the phishing email was not as crisp as the official logo on the bank's website, and the background was slightly different from the original;

If recipients clicked on "Privacy & Security" or "Terms of Use" at the bottom of the fake email, they were directed to the respective page on the legitimate Citizens Bank website. Unless recipients clicked the "back" button immediately after visiting either of the aforementioned pages, they would have soon realized that a "BillPay" page did not exist on the bank's website and that the unsolicited email was a scam.

Never click a link in an unsolicited email!

Example: Royal Bank Impersonation

Forged logo

Typo

Fake URL



Recognize and Avoid Phishing Scams

While it can be difficult to spot a phishing scam at first glance, it is important to be aware of common tactics and characteristics that define them. Here's how you can recognize phishing emails and avoid being taken - hook, line and sinker:

1) Read emails carefully!

Busy schedules are a phisher's dream. Many email users read messages and click on links in the blink of an eye, but it's important to take the time to analyze every email. A few extra minutes now can save you time and money in the future.

2) Never authenticate by email

Never reveal your user identification and/or password in an email! Legitimate enterprises and institutions will never ask you to divulge confidential information, such as passwords and credit card information other than on their official website. If you are asked to provide such details in an email, you are very likely being phished and should close the message immediately and, if possible, report the phishing attempt to the proper authorities (see appendix).

3) Careful what you click

Be wary of links provided in unsolicited emails. Phishing scams instruct you to click on a link that may look legitimate but that leads to a fraudulent website. The web page or site you'll end up on has been purposely designed to look official and aboveboard - but isn't.

4) Never follow a link in an unsolicited email

The best advice is to never click on a link in an unsolicited email. There are two good ways to confirm whether a link is legitimate without clicking on it. First, open a new Internet browser window. Then type in the official web address of the enterprise or financial institution mentioned in the email. Once on the official homepage, look for the specific page identified by the link in the email. Do so by placing the cursor after the last character in the address bar and then typing in the remaining characters. If a corresponding page pops up, the link is legitimate; otherwise, you may get a "404 Error" message, which means the link is fraudulent and the email should be deleted immediately. A second method is to hover your mouse pointer over the link in the email - but don't click on it. Look at the address that appears at the bottom of your screen; if it matches the corresponding link in the email, it may not be fraudulent. However, it is best not to click on a link if there is ANY doubt. If the addresses do not match, someone is trying to fool you - don't click on the link. Just delete the email!

Important alert!

Don't copy & paste to save time!
When directed to a web page in an unsolicited email, never copy and paste the entire link provided.

To avoid ending up on a fraudulent website, type in the homepage URL, then search the website for the page related to the topic in the email you received.

5) Look for security indicators

If you find yourself on a website or web page and are unsure about its authenticity, look for indicators that it is encrypted. These can include a lock icon on the status bar of your browser or a URL beginning with https:// (the "s" stands for "secure"). However, no indicator is foolproof; phishers can forge security icons and create fake secure URLs. If you doubt an email's legitimacy, the best course of action is to exit immediately.

6) Don't act hastily

If an unsolicited email instructs you to authenticate yourself or act immediately to avoid a penalty or other negative consequence...wait. Phishing scams have a short life span. The longer they exist, the greater the chance of detection; this is why phishing emails urge you to act quickly, not because you will actually be penalized by the enterprise or institution that allegedly sent the email.

Waiting a few days or even a week will help you to determine if an email is legitimate. If you haven't responded within that time frame, a legitimate enterprise or financial institution will follow up with you in a letter or phone call.

7) Verify by telephone

If you have any doubts about the legitimacy of an unsolicited email, contact the enterprise or financial institution in question using a phone number that you know is valid. You can obtain this information online or in a printed telephone directory; never automatically trust a phone number, address or any other information provided in an unsolicited email.

8) Secure your inbox/network

Equip yourself with comprehensive email security. Leading email security solutions like Vircom's Modus™ server and gateway products offer a wide range of tools and technology - including Sender Policy Framework (SPF) - to eliminate virtually all phishing scams before they ever reach your inbox.

Never click a link in an unsolicited email!



Do not take any email at face value which asks for personal or confidential information

The SPF authentication protocol specifies which computers are authorized to send email from a particular domain. Email servers that implement SPF reject all emails whose domain names cannot be validated against the Internet Protocol address listed in the corresponding DNS records.

If a phisher has a legitimate account with a specific domain name or owns the domain, he or she can still send email; however, doing so makes the scam much easier to trace and prosecute because it reveals more information about the scammer's location. Since over 95% of all spam comes from hijacked or forged domain names, SPF makes it more difficult for phishers to remain undetected: if they forge the 'from' address of a domain that employs SPF, the spoofed address will not be accepted by the server.

9) Report any suspicious email

Report suspected abuse of your personal information to the proper authorities. This could be as simple as contacting your Internet Service Provider or a government entity that manages cyber crime. Ultimately, it is every email user's individual decision whether or not to respond to an unsolicited email. However, a bit of caution goes a long way; if you receive an unsolicited email requesting banking or credit card information, it is best not to reply to the sender or click on any links in the email (see appendix for a list of reporting resources).

A Final Note on Phishing

Email phishing cannot be eradicated overnight. However, we can all do our part to fight it, one email at a time.

There are countless organizations and enterprises - including Vircom - dedicated to combating email abuse and developing tools and technology that safeguard networks and protect email users from email-borne threats.

Vircom white papers are meant to educate and empower readers. We hope this paper enables readers to make informed decisions that lead to the elimination of phishing attacks. For more information on how Vircom's Modus™ products and services help to combat spam and email fraud, please visit www.vircom.com.

Recap: Reflexes to Acquire

To further emphasize the threat that fraud and phishing emails represent, let us review the proper steps for properly and safely handle unsolicited fraudulent messages:

1. DO NOT CLICK ON ANYTHING in the message. In fact, don't even open the email if you doubt its legitimacy. If you feel compelled to open the email, do so without clicking on any links, buttons, images or anything else.
2. To verify the information in an email, OPEN A NEW WEB BROWSER WINDOW AND TYPE IN THE ADDRESS YOURSELF. Type only the main URL of the organization (e.g. www.mastercard.com), then access your personal account. If there is important information you should know, it's going to be there. If you want to double-check that there is nothing wrong with your account, browse the website or search for the specific topic mentioned in the suspicious email.
3. As soon as you suspect that the email you have received is a phishing attempt, CLOSE IT AND DO NOT REOPEN IT. Vircom strongly suggests that you report phishing attempts to law enforcement authorities and to the impersonated organization.

Norman solutions for clients/workstations: Norman Virus Control for Windows 95, 98, Me, NT4.0, 2000, XP, OS/2, Linux (On-Demand scanning)
• Norman Internet Control for Windows 95, 98, Me, NT4.0, 2000, XP • Norman Personal Firewall • Norman Ad-Aware

Norman solutions for servers: Norman Virus Control for Microsoft Windows NT4.0, 2000, 2003 • Norman Virus Control Firebreak for Novell Netware 4.11 and later • Norman Virus Control for Linux • Norman Virus Control for OS/2

Norman solutions for web/gateways/mailservers: GFI MailEssentials • GFI MailSecurity • GFI DownloadSecurity • NVCnet • Norman Virus Control for Lotus Domino (Win32, OS/2) • Norman Virus Control for Firewall-1 NG • Norman Virus Control for Microsoft Exchange • Norman Virus Control for Microsoft Exchange 5.5 • Norman Virus Control for MIMESweeper



NORMAN[®]
www.norman.com