The Second Generation of Phishing: E-mails no Longer Required

Simply Entering a Bank-related Web Address Could Take You on a Phishing Trip!

"We have discovered that someone has used your Visa card number, which could happen if you have been shopping on-line. To avoid this from happening again, we strongly recommend you fill in the forms on our company website and install the Zero Liability program, in order to quickly investigate this accident.

	http://www.usa.visa.com
	/ /
Visa USA Personal Pro	
	🔏 😧 Search 🚡 Favorites 🎯 History 💁 📾 🖬 🚍 😤 🏦 🏶 🐄
Address 🙋 http://www.usa.vis	
VISA	
1.54	Home Personal Businer
Cards	Shopping & Travel Visa Student Practical Money Skil
Secure with Visa Complete Protection	
Zero Liability	Protect Your Card
Online Protection	
Verified by Visa	With cardholder protection programs such as Zero Liability, Verified by Visa, and BBBOnLine, you can feel safe and secure knowing Visa's got you
Secure Commerce Program Security Tips: Web & Email	covered.
Protection Basics	Please, do not use your credit card after applying for our Zero Liability
Lost Your Card?	program until you will be informed of success. It will take 3-5 business days.
Protect Your Card ATM Safety	
Identity Theft	Your First Name:
Shortcuts	Your Last Name: Your Credit Card Number:
Get a Card	CVV2/CVC Code:
	PIN (ATM Code):
	Select Openium
	Your Credit Card Type:
	Expiration Date: 01 Jan 💌 2004 💌
	Please, ensure all information is correct before submitting the form to avoid any mistakes while processing.
	Protect your Credit Card Now

<u>The fake Visa website is difficult to identify; even the website</u> address is exactly the same as the authentic site. (The webpage above is a fake; the one below is real. The above picture is the site shown by January's HTML_VISAFRAUD.A.)



By clicking on the Continue in this HTML message, a webpage that looks exactly like the original appears, waiting for you to take the bait (see picture). This is HTML VISAFRAUD.A, one example of a malware that has been using the Visa name to deceive victims since January of this year. This kind of 'Phishing' has become a common phenomenon over the last year. This form of fraud is used to steal the personal information of email users, including ID numbers, ATM codes, credit card numbers and more. These emails use the names of well-known companies to warn unsuspecting customers and urge them to visit a fake website to enter their personal information. As these fake websites often look just like the actual websites, many victims have been fooled, unwittingly entering their information. In addition. personal oftentimes the larger the bank, the more

people fooled.

In its early days, phishing was mainly conducted in English, with numerous grammatical errors, and users could avoid falling into their trap as long as they did not click on the link in the message. However, it is now much harder to recognize fraudulent emails; in fact, emails are not always used as bait anymore. What is happening now can be called the second generation of phishing. Trend Micro Trendlabs, a global antivirus research and support center of Trend Micro, has detected a new Trojan horse virus, <u>TROJ BANCOS.CP</u>, which monitors the browsing actions of Internet Explorer in order to record the victim's browsing behavior. Once the title of the Internet Explorer window matches specified banking-related strings, a login page that looks genuine is produced, asking for the user's sensitive information, such as passwords. This secretly recorded information is stored in a special folder, and is then automatically sent to hackers via email. After this information is sent, the folder is automatically deleted in order to avoid leaving any tracks. It is very possible that a victim's information is stolen without the victim ever knowing.

TrendLabs explains that this is very different from phishing of the past, when they simply consisted of fraudulent letters seemingly from banks. Most internet users could easily identify those fraudulent phishing emails from their grammatical errors. However, users now need only enter a bank's website address to fall victim. TrendLabs points out that there are currently eighty variants of TROJ_BANCOS, the newest of which logs keystrokes, collects data and even print screen, then it sends those stolen information to the virus author.

CAIXA	INTERNET BANKING CAIXA
Login Tipo: 001 - Conta Corrente - Agência: Conta: Senha Internet:	P.Física ▼ ! 1 2 # 3 5 4 % 5 6 & 7 * 8 (9)0 - + = ← Q W E R T Y U I O P `, {[slock A S D F G H J K L Ç ^}] i \ Z X C V B N M <
you enter a bank-related string nal information.	specified by TROJ_BANCOS, a fake website will appear asking

Trend Micro shows an easy way to identify such sites: legitimate HTTPS website must display the padlock icon in the status bar. When a website address begins with HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer), it signifies that a Secure Socket Layer is added to the HTTP address, making it difficult for HTTP documents to be intercepted during transmission over the internet. Therefore, the address for most websites asking for personal information will begin with HTTPS. However, this address itself is not very difficult for hackers to copy, so users must also check to see if the padlock icon is displayed in the lower right corner of the window.

In the Citibank phishing case, the link takes you to what looks like a valid Citibank website, with an address that begins with Https. However, while it looks like a secure site, there is no padlock icon in the lower right corner to verify it as a safe website.

In another example, <u>HTML PAYPFRAUD.A</u> impersonates Paypal, displaying a seemingly real registration page with legitimate web address of Paypal, but the login page that is actually shown is a fake. In fact, the login page used by Paypall users is not the site's homepage; in addition, the login page displays the padlock icon, which the fake website does not.

Identify	Your Verifi	ication - Microso	oft Interne	t Explorer			- 🗆 ×
<u>E</u> ile <u>E</u> dit	<u>V</u> iew F <u>a</u>	vorites <u>T</u> ools	<u>H</u> elp				
e , Back	. 🔶 Forward	- 💌 Stop	C Refresh	Home	Q Search	I	**
A <u>d</u> dress	http://wwv	v.paypal.com			•	¢∂Go	Links »
Per	Pal	0					
Welc	ome	Send Money	Req	uest Mon	ey 🛛	Merch	iant ⁻
Persor	nal Ac	count Ide	entity '	Verifica	ation	l - Jus	t 1-P
Your Pro	file Info	rmation - Ente	r your nar	ne as it app	ears or	n your	credit
		First Name:					
		Last Name:					
		Address 1:					
		Address 2: (optional) City:	I				
		State:	-				
		Zip:		/		>	
Done				ð 🗌 🚱	Local intr	ranet	
The fake logi	n page of	Paypal – displa	ying home	page addres	ss of Pa	aypal in	the upper
status bar, no	padlock ic	on shown in low	er right cori	ner.			

← → → ⊗ ② ③ ③ » Bad <mark>e Forward Stop Refresh Home Scarehr</mark>	ile Edit	- Sign Up View	Favorites		net Exploi Help	rer				
Bact Howard Sup Kerresh Home Sourch dress https://www.paypal.com/cgi-bin/webscr?_track=_regis Go Links » PERENT Go Links * PERENT GO Links * P			•					6		>>
Welcome Send Money Request Money Merchant CCOUNT Sign Up ersonal Account 1 Enter Your Confirm You 2 Confirm You Dur Address Information - Begin building your profile by entering your redit card or bank account. First Name: Last Name: Address 1: Address 2: (option al) First* Address 2: (authentic login page: the link which appears is actually not the homepage addressed of the set of the		- Form	and 🔻	Stop		Home		- earch		
Address 1: Address 1: Address 2: (optional) Fitze: authentic login page: the link which appears is actually not the homepage address	<u>i</u> dre:s 🧕	https://	www.payp	al.com/cgi	-bin/websc	r?_track	=_regis	- 6	Go	Links »
Address 1: Address 1: Address 2: (optional) Fitze: authentic login page: the link which appears is actually not the homepage address										
Address 1: Address 1: Address 2: (optional) Fitze: authentic login page: the link which appears is actually not the homepage address	PETY	Pal	*							
Address 1: Address 1: Address 2: (optional) Fitze: authentic login page: the link which appears is actually not the homepage address	Wole		Fond	Monou	Bac	uoct M			larch	ant 7
ersonal Account 2 Confirm You our Address Information - Begin building your profile by entering your redit card or bank account. First Name: Last Name: Address 1: Address 2: (option al) Fity: e authentic login page: the link which appears is actually not the homepage addr	weici	Jine	Sellu	Money	Ret	luest M	uney	W	ercii	
ersonal Account 2 Confirm You our Address Information - Begin building your profile by entering your redit card or bank account. First Name: Last Name: Address 1: Address 2: (option al) Fity: e authentic login page: the link which appears is actually not the homepage addr										
Address 1: Address 2: (option al) Fity: authentic login page: the link which appears is actually not the homepage addr	rersoi	nal Δ	ccoun	it.				2 Co	ofiro	N YOU
Address 1: Address 2: (option al) Fity: authentic login page: the link which appears is actually not the homepage addr	our Add	lress II	n formati ik accoun	i on - Beg t.	in buildir	ig your (orofile I			
Address 2: (option al) Fity: authentic login page: the link which appears is actually not the homepage address and the homepage address at the homepage at the home	our Add	lress II	nformati Ik accoun First	i on - Beg t. : Name:	jin buildir	ig your (profile I			
(option al)	our Add	lress II	nformati ik accoun First Last	ion - Beg t. : Name: : Name:	in buildir	ng your (orofile I			
authentic login page: the link which appears is actually not the homepage addr	our Add	lress II	nformati ik accoun First Last Add	ion - Beg t. : Name: : Name: Iress 1:	jin buildir	ng your (orofile I			
e authentic login page: the link which appears is actually not the homepage addr	our Add	lress II	nformati ik accoun First Last Add Add	ion - Beg t. : Name: : Name: Iress 1: Iress 2:	jin buildir	ng your (profile I			
e authentic login page: the link which appears is actually not the homepage addr	our Add	lress II	nformati ik accoun First Last Add Add	ion - Beg t. : Name: : Name: Iress 1: Iress 2: optional)		ng your (profile I			
	our Add	lress II	nformati ik accoun First Last Add Add	ion - Beg t. : Name: : Name: Iress 1: Iress 2: optional)		ng your (2	by ent		
/bal, in addition, padlock icon is there.	redit card	lress In	nformati k accoun First Last Add (c	ion - Beg t. : Name: : Name: Iress 1: Iress 2: optional) City:			o Inte	ernet	ering	your
	redit card	lress In	nformati k accoun First Last Add (c	ion - Beg t. : Name: : Name: Iress 1: Iress 2: optional) City:			o Inte	ernet	ering	your

Security specialists appeal to internet users to employ an antivirus program that blocks phishing websites, such as Trend Micro's PhishTrap. This program actively stops users from accessing fraudulent websites and preventing them from downloading malware, including phishing websites with complicated script programs and those that avoid HTTP filter scanners.

Report phishing mails to: antifraud@support.trendmicro.com

Internet security specialists Trend Micro: www.trendmicro.com