

## Presents



# Scammer! The "Roger" Report

Help prevent scams and fraud. Please share this with everybody! The more people who read this report, the fewer the number of people who will fall for this type of scam in the future.



You have probably heard of the "Microsoft scam", where you receive a telephone call from someone purporting to be from Microsoft who tells you that your computer is infected. The caller tells you that it is necessary for you to have your computer cleaned immediately, a service he is happy to provide for a small fee. He can do this by remotely logging into your computer.

Of course, Microsoft NEVER calls users to inform them that their computer is infected. If you grant the caller access to your computer, he will likely infect your computer with malicious software designed to capture information enabling him to access your bank account and charge cards, and do anything else he desires.

Recently, I received a call from "Roger" who works at "Technical Department".

*Roger:* "Your computer is infected, you need to clean it right away." *Me:* "Oh no, that doesn't sound good, what should I do?" *Roger:* "No problem sir, I can take care of it for you from remote".

Of course, my computer was not infected. The only one that might call you to tell you that your computer is infected is your Internet provider, and they won't offer to fix it for you from remote. They will tell you to take it to a professional computer shop (like McLean Micro) and have it properly fixed.

Fortunately, I had a virtual machine ready that I could grant him access to. If you don't know what a virtual machine is, it is a fake computer that runs in a window on your real computer. It runs its own copy of Windows, and can be completely isolated from the real computer.

I was able to observe everything he did, and capture video and screen shots. And since I am a computer/network technician at McLean Micro (and pretty good at my job), I was able to fool "Roger" and make him believe what I wanted him to.

During our remote sessions (which spanned several weeks), "Roger" often



put me on hold to consult with his "senior technician", or his "accounts manager".

When he "puts me on hold", I'm not really on hold, I can hear what is going on at the "technical center". It sounds like there are many people working there, under the direction of one or more supervisors.

It is obvious that "Roger" is working from a script, and when anything happens that he doesn't know how to deal with (for example, when the "customer" doesn't have a charge card), he asks someone else what he is supposed to do. "Roger" appears to have little technical skill, and he (and his superiors) are easily fooled.

You might ask why I would want to bother wasting my time with "Roger" instead of just hanging up. There are a number of reasons:

- I wanted to see exactly what these scammers do when they access your computer from remote.
- When they are trying to scam me, they aren't scamming someone who is unable to spot and deal with this type of scam.
- I may be able gather information that could be of help to law enforcement in preventing this type of scam in the future (or, as was the case here, try to help someone being scammed right now).
- It can be fun to outsmart a scammer like "Roger", there were a couple of times when I had to cover the mouthpiece on the phone, so he wouldn't hear me laughing.

If you're going to try to scam someone who is smarter and more technically competent than you are, you aren't going to win. Just ask "Roger".

Note that when I refer to "Roger", I am referring not only to the voice I hear on the phone, but to the person or persons who are accessing my computer from remote. I believe that the "Roger" I hear on the phone is merely the voice the victim hears, and that much of the remote work is done by someone else.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

🖉 LogMeIn123.com - Remote Support - Windows In	ternet Explorer		
Https://secure.logmeinrescue.com/Customer	/Code.aspx	💌 🔒 🐓 🗙 🔁 Bing	P -
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp			
🛧 Favorites 🛛 👍 🙋 Suggested Sites 👻 🔊 Free Hotmail	🖉 Web Slice Gallery 🝷		
C LogMeIn123.com - Remote Support		🔓 • 🗟 • 🖃 🖶 •	Page • Safety • Tools • 🕢 *
C LogMeIn Rescue			
k I	Support Connectio	n	
	Enter your 6-digit code		
	How It Works ()		
	We take security seriously, <u>Report Ab</u>	<u>use</u>	
	Copyright © 2005-2013 LogMeIn, Inc. All rights reserved. Le		
Done		😜 Internet	🖓 🔹 🔍 100% 👻 🛒
Start / LogMeIn123.com - R		2	l 📮 觰 🖲 🕲 🧐 🏂 8:49 PM

## Session One

The first thing a scammer needs is access to your computer. "Roger" directed me to a site, secure.logmeinrescue.com, where I would download a utility granting "Roger" remote access to my computer.

Since I had a virtual machine ready, that is what I granted him access to.

To clarify, the sections "Session One" or "Session Two" etc, are not consecutive days, and they are not my only phone conversations with "Roger". They are only days when I allowed him remote access to my "computer".



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

CLogMeIn Rescue - Remote Access Software and	Remote Control Software - Windows Internet Explorer	
COC - O https://secure.logmeinrescue.com/Custon	er/TrialWarning.aspx?code=950218	P -
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp		
🚖 Favorites 🛛 🚖 🙋 Suggested Sites 🝷 🙋 Free Hotma	l 🖉 Web Slice Gallery 👻	
OLogMeIn Rescue - Remote Access Software and Rem		age $\star$ Safety $\star$ Tools $\star$ $@\star$
C LogMeIn Rescue		
	Be cautious taking unsolicited calls for support. Only accept support from people you trust. This technician is using a trial version of LogMeIn Rescue.	
	Copyright © 2005-2013 LogMeIn, Inc. All rights reserved. <u>Legal</u> <u>Sales</u>	
https://secure.logmeinrescue.com/Customer/TrialWarning.aspx		🖓 🔹 🔍 100% 🔹 🏢
🛃 start 🧷 🥭 LogMeIn123.com – R		🖡 🚯 🕲 🧶 🗞 8:50 PM

I didn't ask "Roger" about the warning that popped up when I ran the remote access utility, I didn't want to ask him too many questions he couldn't answer.

If he knew he wasn't scamming me, he would have disconnected.

LogMeInRescue is a legitimate service that allows IT people to log into their clients computers from remote to fix minor issues. It can also be used by scammers to access your computer, **but only if you let them.** 



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

1									
Recycle Bin		Event Viewer							
		File Action View Help							
		ALL							
			<u> </u>						
		Event Viewer (Local)	System 409 e						
		Application	Туре 🗸	Date	Time	Source	<u>^</u>		
		System	S Error	8/20/2013	6:17:03 PM	W32Time			
		System	Error	8/20/2013	6:17:03 PM	W32Time	_		
		_	Error	8/20/2013	6:17:06 PM	W32Time			
			Error	8/20/2013	6:17:06 PM	W32Time			
			Error	8/20/2013	6:23:23 PM	W32Time			
			Error	8/20/2013	6:23:23 PM	W32Time			
			Error	8/20/2013	6:23:26 PM	W32Time			
			Error	8/20/2013	6:23:26 PM	W32Time			
			🛛 🙆 Warning	10/4/2011	9:12:29 PM	Print			
			Warning	10/4/2011	9:12:31 PM	Print			
			🛛 🙆 Warning	10/4/2011	8:59:36 PM	Dhcp			
			Warning	10/4/2011	8:59:46 PM	Dhcp			
			Warning	8/20/2013	6:16:56 PM	Dhcp			
			🛛 🔔 Warning	8/20/2013	6:23:17 PM	Dhcp			
			Information	10/4/2011	4:50:30 PM	eventlog			
			Information	10/4/2011	4:50:30 PM	eventlog			
			Information	10/4/2011	4:50:11 PM	serial			
			Information	10/4/2011	4:50:11 PM	serial			
			Information	10/4/2011	8:58:04 PM	eventlog			
			Information	10/4/2011	8:58:36 PM	Workstation			
			Information	10/4/2011	9:04:35 PM	Http			
			Information	10/4/2011	9:07:47 PM	Setup			
			Information	10/4/2011	9:09:14 PM	eventlog	-		
			Information	10/4/2011	9:09:14 PM	eventlog	<u>×</u>		
			<				>		
		a							
	100								
🦺 start 🔰	(Trial version) HP	📑 Event Viewer					2 🗘	🔏 🛈 🕲 ગ 🏷	9:06 PM
		ALCONDUCT T						and the second	

"Roger" opened my event viewer and explained that the red errors were caused by viruses and infections.

*Roger:* "Each of these red and yellow marks are thousands of infections, this is bad. Very very bad."

In reality, the virtual machine was a fresh install. A certain number of errors and warnings in the event logs are normal (depending on the error or warning) and there was nothing wrong with the computer.

Note in the taskbar that the remote access software is the trial version of HP Care (which uses LogMeInRescue).



#### Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

🖉 [Invalid] Markup Validation	of http://ww	w.google.ca/ - W3C Marku	p Validator - Windows Int	ternet Explorer	- 7
COO - Mainter://validator.wa	3.org/check?uri=	=www.google.ca&charset=%28d	etect+automatically%29&doctyp	pe=Inli 🔽 🗟 🍫 🗙 🔽 Bing	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ool	ls <u>H</u> elp				
🚖 Favorites 🛛 🚔 🔊 Suggested S	Sites 🔹 🙋 Free	e Hotmail 🙋 Web Slice Gallery 🛛	•		
[Invalid] Markup Validation of http:	://www.google.c	a/		🏠 🔹 🔝 👻 📇 👻 <u>P</u> age 🕶	Safety + Tools + 🕢 *
Ma Ma	arkup \	/alidation Serv	vice	R	- The second
Chec	ck the markup	(HTML, XHTML,) of Web	documents		
		Jump To: Notes a	and Potential Issues	Validation Output	
	Er	rors found while	checking this doc	ument as HTML5!	
R		7 Errors, 4 warning(s)	9		
Add	dress :	http://www.google.c	a/		
Enco	oding: is	6-8859-1	(detect automatically)	×	
Doc	ctype : H	TML5	(detect automatically)	×	
Root Ele	ement: h	tml			
	The W30	C validators are hosted	on server technology d	onated by HP, and supported by communi	ty
תה)			donations.		4000
		Donate a	and help us build better	tools for a better web.	🖾 Flattr
Options					
					✓
Done	T	0		🛞 🚱 Internet	🗛 🔹 🔍 100% 🔹 📑
🛃 start 🔰 📃 Computer M.	lanagement	(Trial version) HP Care	🜈 [Invalid] Markup Valid	2 🗘	📵 🕲 🧐 🏷 8:21 PM

Next, "Roger" opened my browser (Internet Explorer) and went to an HTML validation page. He entered the Google home page in the validator, which generated a number of errors and warnings.

These, he explained, were further indications of the severity of the infections in my computer.

Obviously, any HTML errors on the Google home page have nothing whatsoever to do with my computer. I didn't ask "Roger" about this, I was pretending to be technically challenged, so played along to see what would happen next.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca



Now "Roger" transfers software to my computer, and installs and runs it.

I have never heard of "Advanced WindowsCare 2", but I do know that a fresh install of Windows isn't going to have thousands of problems. The virtual machine I allowed "Roger" to access had never even been on the Internet, except to activate the Windows.



💽 🗢 🙋 http://hpcare.webs.com/rates-and-servi	ices	🖌 🗲 🔀 Bing	2
e <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>I</u> ools <u>H</u> elp			
Favorites 🛛 👍 🕖 Suggested Sites 🝷 💋 Free Hotm	ail 🙋 Web Slice Gallery 👻		
hpcare - Rates And Services		🟠 🔹 🔝 👘 🖃 🖶 🍷 Page 🔹 Safety 🔹 Tools 🔹	<b>?</b> -
	Optimizing your PC's speed and Perfor	Diagnostic & repair of your software issues. Troubleshooting software errors. Updating drivers and security to protect against online threats. Connecting to the Internet, devices and peripherals.	
	a) Clear Internet Cache Files b) Clear Browser History and Cookies c) Clear Temporary Windows Files d) Clear Recent Windows Files e) Clear Temp Folder f) Clear Prefetch		
	<ul> <li>g) Clear Event Log</li> <li>h) Clear Recycle Bin</li> <li>i) Clear Clip Board</li> <li>2.System Diagnostics</li> <li>a) Check your Disk</li> <li>b) Scan and Fix System Files</li> <li>c) Check your Disk Space</li> <li>d) System Info</li> <li>e) Port Scan</li> </ul>		3
	f) Disk Defragmentation	SOFTWARE PROTECTION	)% •

After poking around my system for a few minutes, including looking at my system properties, and doing some useless things at a command prompt (no doubt to convince me of the level of infection on my computer and of "Roger's" ability to correct them), we wind up at a page where I can purchase "services" to fix my system.

These "services" include (among other things) emptying my recycle bin, and clearing my clip board, all for the bargain price of \$199. And it even includes lifetime support! But as you will see later, if you fall for the scam, they may be able to steal far more than the initial payment from you, and do so without any further help from you.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

Edit View Favorites Iools Help Favorites Suggested Sites C Free Hotmall Web Site Gallery C Canada moving money for better WESTERNIC MUSSERN Canada moving money for better Western Union Location < Return to Results Print Share MONEY MART #0648 85 Prince Edward St Saint John, NB E2L 3S1 506-636-8574 Schedule for next 7 Days Monday 9:00 AM - 9:00 PM Tuesday 9:00 AM - 9:00 PM Tuesday 9:00 AM - 9:00 PM Thursday 9:00 AM - 9:00 PM Saturday Closed Services	About Us Investor Relations   Transfer Status   Contact Us   Help Canada Sign In Register   Consumer Services Find a Location	
<ul> <li>✓ Phpcare - Rates And Services</li> <li>✓ WESTERNIC moving money for better</li> <li>✓ Western Union Location</li> <li>&lt; Return to Results</li> <li>✓ Print Share</li> <li>MONEY MART #0648</li> <li>85 Prince Edward St Saint John, NB E2L 3S1 506-636-8574</li> <li>✓ Schedule for next 7 Days</li> <li>Monday 9:00 AM - 9:00 PM</li> <li>Tuesday 9:00 AM - 9:00 PM</li> <li>Tuesday 9:00 AM - 9:00 PM</li> <li>Thursday 9:00 AM - 9:00 PM</li> <li>Saturday Closed</li> <li>Sunday Closed</li> </ul>	About Us   Investor Relations   Transfer Status   Contact Us   Help	
WESTERNIC       Canada         moving money for better       Western Union Location         Vestern Union Location           Return to Results       Print       Share         MONEY MART #0648       85 Prince Edward St       Saint John, NB E2L 3S1       506-636-8574         Schedule for next 7 Days       Monday       9:00 AM - 9:00 PM       Yuesday       Yuesday       9:00 AM - 9:00 PM         Tuesday       9:00 AM - 9:00 PM       Thursday       9:00 AM - 9:00 PM       Thursday       9:00 AM - 9:00 PM         Friday       9:00 AM - 9:00 PM       Saturday       Closed       Sunday       Closed	About Us   Investor Relations   Transfer Status   Contact Us   Help	
Canada         moving money for better         Canada         Western Union Location         < Return to Results       Print       Share         MONEY MART #0648       85 Prince Edward St       Saint John, NB E2L 3S1       506-636-8574         Schedule for next 7 Days         Monday       9:00 AM - 9:00 PM         Tuesday       9:00 AM - 9:00 PM         Thursday       9:00 AM - 9:00 PM         Friday       9:00 AM - 9:00 PM         Saturday       Closed         Sunday       Closed	Canada 💽 English 💟	
Canada         moving money for better         Canada         Western Union Location         < Return to Results		
moving money for better         Western Union Location         < Return to Results	Sign In Register Consumer Services Find a Location	
< Return to Results		
< Return to Results Print Share MONEY MART #0648 85 Prince Edward St Saint John, NB E2L 3S1 506-636-8574 Schedule for next 7 Days Monday 9:00 AM - 9:00 PM Tuesday 9:00 AM - 9:00 PM Tuesday 9:00 AM - 9:00 PM Thursday 9:00 AM - 9:00 PM Thursday 9:00 AM - 9:00 PM Friday 9:00 AM - 9:00 PM Saturday Closed Sunday Closed		
MONEY MART #0648 85 Prince Edward St Saint John, NB E2L 3S1 506-636-8574 Schedule for next 7 Days Monday 9:00 AM - 9:00 PM Tuesday 9:00 AM - 9:00 PM Wednesday 9:00 AM - 9:00 PM Thursday 9:00 AM - 9:00 PM Friday 9:00 AM - 9:00 PM Saturday Closed Sunday Closed		
MONEY MART #0648 85 Prince Edward St Saint John, NB E2L 3S1 506-636-8574 Schedule for next 7 Days Monday 9:00 AM - 9:00 PM Tuesday 9:00 AM - 9:00 PM Wednesday 9:00 AM - 9:00 PM Thursday 9:00 AM - 9:00 PM Friday 9:00 AM - 9:00 PM Saturday Closed Sunday Closed		
85 Prince Edward St Saint John, NB E2L 3S1 506-636-8574 Schedule for next 7 Days Monday 9:00 AM - 9:00 PM Tuesday 9:00 AM - 9:00 PM Wednesday 9:00 AM - 9:00 PM Thursday 9:00 AM - 9:00 PM Friday 9:00 AM - 9:00 PM Saturday Closed Sunday Closed		
Saint John, NB E2L 3S1 506-636-8574 Schedule for next 7 Days Monday 9:00 AM - 9:00 PM Tuesday 9:00 AM - 9:00 PM Wednesday 9:00 AM - 9:00 PM Thursday 9:00 AM - 9:00 PM Friday 9:00 AM - 9:00 PM Saturday Closed Sunday Closed		
506-636-8574           Schedule for next 7 Days           Monday         9:00 AM - 9:00 PM           Tuesday         9:00 AM - 9:00 PM           Wednesday         9:00 AM - 9:00 PM           Thursday         9:00 AM - 9:00 PM           Friday         9:00 AM - 9:00 PM           Friday         9:00 AM - 9:00 PM           Saturday         Closed           Sunday         Closed		
Schedule for next 7 DaysMonday9:00 AM - 9:00 PMTuesday9:00 AM - 9:00 PMWednesday9:00 AM - 9:00 PMThursday9:00 AM - 9:00 PMFriday9:00 AM - 9:00 PMFriday9:00 AM - 9:00 PMSaturdayClosedSundayClosed		
Schedule for next 7 DaysMonday9:00 AM - 9:00 PMTuesday9:00 AM - 9:00 PMWednesday9:00 AM - 9:00 PMThursday9:00 AM - 9:00 PMFriday9:00 AM - 9:00 PMSaturdayClosedSundayClosed		
Monday         9:00 AM         9:00 PM           Tuesday         9:00 AM         9:00 PM           Wednesday         9:00 AM         9:00 PM           Thursday         9:00 AM         9:00 PM           Friday         9:00 AM         9:00 PM           Saturday         0:00 AM         9:00 PM           Sunday         Closed         0		
Tuesday 9:00 AM - 9:00 PM Wednesday 9:00 AM - 9:00 PM Thursday 9:00 AM - 9:00 PM Friday 9:00 AM - 9:00 PM Saturday Closed Sunday Closed		
Wednesday 9:00 AM - 9:00 PM Thursday 9:00 AM - 9:00 PM Friday 9:00 AM - 9:00 PM Saturday Closed Sunday Closed		
Thursday 9:00 AM - 9:00 PM Friday 9:00 AM - 9:00 PM Saturday Closed Sunday Closed		
Friday 9:00 AM - 9:00 PM Saturday Closed Sunday Closed		
Saturday Closed Sunday Closed		
Sunday Closed		
Services		
Services		
Payments		
Quick Collect		
Money Order		
Money Transfer		
Mobile Money Transfer		
Money Transfer to a Bank Account		
one	🛞 🗐 Internet	🐴 🔹 🔍 100%

*Me:* "But Roger, I don't have a charge card, what can I do?" *Roger:* "Let me put you on hold while I talk with my accounts manager."

Roger: "Ok, I need you to go to Western Union, and send a money transfer."

Payment will be made to the "accounts manager". Accounting, he explained, has been "outsourced to India", so that is where I will have to send the payment.

"Roger" trusts me, so he will begin the service immediately.





"Roger" installs more software on my system, then does a disk defragment (which runs very quickly in a virtual machine), and runs the disk cleanup wizard.

"Roger" doesn't need me at this point, so we hang up while "Roger" continues to work from remote.

I told him I was going to bed, but of course I was watching (and recording) everything he did.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

Select the records you want to intercept	
Computer Activity Subject	60       minutes         aid       singh.raj02@yahoo.com         t       Log File         ar       singh.raj02@yahoo.com         st       smtp.mail.yahoo.com
	Wizaru
	Hide everywhere Hide icon from tray Hide the program with Ctrl+Alt+Del Remove shortcut from DESKTOP Remove shortcuts from START MENU A Remove shortcuts from START MENU Cancel

Now "Roger" installs software that will monitor everything anyone does on the computer. It reads every key you type, records every web site you visit, every file you open, and everything else you do.

He sets it to email the log file every 60 minutes, and to hide in the system so it is undetectable.

Using this, "Roger" can capture banking and charge card information, passwords, and everything else that is done on the computer. He can (and will) use this information to steal money from the victim's charge card and/or bank account.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

vi		-1	_			
Recycle Bin C:\WINDOWS\system32\cmd	l.exe _ 🗖	×				
04/14/2008         08:00 AM           04/14/2008         08:00 AM	54,764 Senumal1.011 39,424 sens.dll 7,168 sensapi.dll 13,824 senscfg.dll 14,336 serialui.dll 56,320 services.dll 110,592 services.msc 33,464 services.msc 14,848 servidru.dll 141,312 sessmgr.exe 31,232 sethc.exe (DIR) Setup 240,120 setub.bmp	m		Capacity 39,99 GB	Free Space 35.95 GB	% Free Sp 8
04/14/2008         08:00 AM	23,040 setup.exe 985,088 setupapi.dll 414,208 setupall.dll 32,768 setupn.exe 11,753 setver.exe 5,120 sfc.dll 9,728 sfc.exe 1,614,848 sfcfiles.dll 140,288 sfc_os.dll 23,552 sfmapi.dll SOFTWARE SUPPORTT - Notepad Elle Edit Format View Help	-				
	Sir / mam SOFTWARE PRO ACTIVATION IS RUNNING I PLEASE DO NOT TOUCH THE KEYBOARD OR HAMPER THE ACTIVATION					
	THANKS					
	SUPPORT TEAM					
	Sir					
	Are u there ?					
Start (Trial version) HP Care	(Trial version) hp care		SOFTW	/ARE SUPPO		9:24 PM

"Roger" downloads and runs "Software Pro Activation" on my computer. He explained before that he will install this to help fix my computer, and I should not touch the keyboard or mouse. He puts a note on the screen to this effect.

In reality, "Software Pro Activation" is just a batch file that keeps a directory listing scrolling by forever in a DOS window. Apparently, "Roger" wants the computer to look like it is doing something useful, so I will think he is hard at work earning his money (which, or course, he will never receive).

This runs for a long time. After a while, "Roger" shuts down the computer. He said he would do this when he was done for the night.



#### Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

	http://status.westernunion.ca/track.html		This URL looks real to "Roger".	💌 🗟 🗲 🗙 🔽 Bing	٩
	w Favorites <u>T</u> ools <u>H</u> elp				
avorites	👍 🔊 Suggested Sites 🔻 🔊 Free Hotmail 🌘	🛃 Web Slice Gallery 🔻			
rack a Mone	ey Transfer   Western Union				age + Safety + Tools + 🕢 +
	W0-775 DESTINATION INCOMPLETE				
	MTCN	: 8527742553			
	Transfer Status	: In Transit ON	HOLD		
	Transfer Amount	: \$199.00	HOLD		
	Transfer Currency	: Canadian Dolla	irs		
	Canadam				
	Sender	: Dave MacLaine			
	Sender's Office ID	: Money Mart #06			
	Sender's Office Address	: 85 Prince Edwa	ird St		
	Sender's Office City	: Saint John			
	Sender's Office Country Sender's Office Postal Code	: Canada : E2L 3S1			
	Sender's Ullice Postal Code	: 525 331			
	Receiver	: Tamanna Parvee	n		
	Receiver's Office ID	: MISSING			
	Receiver's Office Address	: MISSING			
	Receiver's Office City	: Kolkata			
	Receiver's Office Country	: India			
	Receiver's Office Postal Code				
		43			
	Funds in the amount of \$199.00 CDN to hold.	o Tamanna Parveen i	in Kolkata India are in transit bu	ton	
	Due to network infrastructure upgrade				
	offices in New Zealand and parts of Ca restriction will be implemented on a w			his	
	Please have the sending office enter a	any information indic	ated above as missing.		
Ple	ase Note: Transactions to certain destinatio	ons may take longer o	r be subject to additional restrict	ions.	
					>
ne				) Internet	🕢 🗸 🔍 100% 🔹
				Theoriet	THE - 100 /0

## Session Two

When "Roger" called the next day, I was again ready for him.

*Me:* "The girl at Western Union said that because of a new network system they have in Canada, I need to tell them more information about where your accounts manager will pick up the money."

Roger: "Ok, let me put you on hold while I check with my accounts manager."

Note the URL above, it appears to point to a valid Western Union page. Actually, it is a fake page on my web server running at home. You can do this type of thing if you are a network technician and run your own web and DNS servers.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

🕼 WESTERN UNION - Notepad	
File <u>E</u> dit Format <u>V</u> iew <u>H</u> elp	
PURPOSEPERSONAL	
10 MTCN NO	
MONEY MART #0648 85 Prince Edward St Saint John, NB E2L 3S1 506-636-8574	
emailhp.care24@yahoo.com	
Cust IDCAN 2023	
Receiver : Tamanna Parveen Receiver's Office ID : Andhra Bank Receiver's Office Address : 101 A B.T Road,kolkata 700090 Receiver's Office City : Kolkata Receiver's Office Country : India Receiver's Office Postal Code : KOLKATA 700090	
SHOPPERS DRUG MART-CANADA POST More Information SHOPPERS DRUG MART-CANADA POST 57 LANSDOWNE AVE SAINT JOHN, NB E2K 2Z9 (506) 634-1774	
AWTONS DRUGS-CANADA POST More Information LAWTONS DRUGS-CANADA POST 39 KING ST SAINT JOHN, NB E2L 4W3 (506) 634-1422	~
🗗 Start 💿 🛞 (Trial version) HP Care 👔 WESTERN UNION - N 🚺 WESTERN UNION - N	😰 🌹 文 🖲 🎕 🍇 8:14 PM

"Roger" agrees to provide the required information, and opens notepad to type it in. He tells me to be sure to go back to the Western Union office tomorrow with the information, and complete the transfer.

He says that if there is any problem with Western Union, to send a MoneyGram instead, and he finds two locations (the post offices in Shoppers Drug Mart and Lawton Drugs) where I can do this.

He explains that I should tell them the transfer is for personal (not business) reasons "to save on the money transfer fee". I thank "Roger" for trying to save me some money. While doing my best not to laugh, I tell him I will take care of it in the morning.



-							
Decycle C		WS\evet	m32\cmd a	Vo			
04/ 04/ 04/ 04/ 04/ 04/ 04/ 04/ 04/ 04/	05/2010 14/2008	WS system 11:549 11:549 0002 12:509 002:509		xe 384,512 mp4sdm 118,272 mpeg2d 148,972 mpg2sp 240,640 mpg4dm 262,416 mpg4ds 123,392 mp1ay3 22,016 mpnoti 59,904 mpr-dl 87,040 mprapi 69,120 mprdm 53,248 mprdim 99,840 mprasg 47,104 mprui. 138,240 mgad.d 19,968 mgbkup 10,752 mgcert 47,616 mgdscl 60,928 mggent 16,896 mgise. 89,088 mglogm 225,280 mgoa.t 36,864 mgoa.t 36,865 mgprfs 663,040 mgrd.d 177,152 mgrt.d	.dl1 dl1 ll .exe ui.dl1 i.dl1 r.dl1 dl1 gr.dl1 lb l.tlb .tlb .tlb .tlb .tlb .ll .dl1 .dl1		
Windows-KB bit							
DIC				File Edit Format View	State of the state of the state of the		
				Sir / mam			
				PLEASE DO I		IS RUNNING IN KEYBOARD OR T	
				THANKS			
				SUPPORT TE	AM		
🐮 start	<b>O</b> (1	rial version	n) HP Care	(Trial version) hp care	C:\WINDOWS\syste	SOFTWARE SUPPOR	 🔇 🖲 🗐 獩 8:23 PM

I hang up with "Roger", because he does not need me on the phone as he works from remote, and I tell him I am going to bed.

He runs "Software Pro Activation" again. The directory listing scrolls by endlessly.



2									
		WS\svstem32	\cmd.exe			- 🗆 ×			
WESTER UNION AA_V Software warranty	cx         C: WINDO           04/14/2008         04/14/2008           04/14/20	08:00 AM 08:00 AM 08:00 AM 12:07 PM 08:00 AM 08:00 AM 08:00 AM 08:00 Refo 08:00 08:0	31,232 12,800 90,112 52,224 8,704 93,696 14,848	traffic.dll tree.com trkwks.dll tsbywo.dll tsbywo.dll tscfgwni.dll tscfgwni.dll tscon ave rour trial period ends soon! <b>29 days re</b> You can use the fully function However, certain features are Use "Buy Now!" button to pur continue your trial period. <b>Buy Now!</b> If you already have a registre "Activate":	maining al version of this progi e only available in regis chase you license imm	ram as long as you want. stered version. vediately or click "Buy Late	er" to		
	04/14/2008	08:00		Activate			nd notes		
Windows-KE bit	3								
			REFOG					IPUTER , SO	
			<b>) On-Screen Keyboard</b> le <u>K</u> eyboard <u>S</u> ettings <u>H</u> el;	p		L.		AS IT MAY	
		e	sc F1 F2 F3 F4	F5 F6 F7 F8 F9	F10 F11 F12 ps	sc sik pau			
			12345	67890-	= bksp in				
			tab Q W E R lock A S D F	TYUIOP GHJKL;	[]] \ de 'ent	elendpdn 78 45	9 6 +		
				V B N M	shft	1 2	3		
			ctri 🎝 alt	alt	👌 🗐 ctrl 🔸		. ent		
📲 sta	rt 💽 🕑 🕻	Trial version) HP .	💽 (Trial version) hp c	c C:\WINDOWS\sys	SOFTWARE S	iUPP 📃 On-Scre	en Keyboard	2 🕄 🔇 🖲 🧐 🗞 🕴	33 PM

"Roger" double checks the remote spy software he previously installed (a trial version of employee monitoring software) to see what I have done between calls. I didn't even power on the virtual machine, so there is nothing to report (which is why he didn't get any email from the software).

He then does all the same things he did the previous night, and shuts down the computer when he is done.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

Track a Money Transfer   Western Union - Windows Internet Explorer	🗸 🐼 🚱 😽 🗙 🔽 Bing	<u>کا ٿا</u> ۔ - م
Elle Edit View Favorites Tools Help		
Arrorites Arrorites Suggested Sites • Bree Hotmail B Web Slice Gallery •		
Track a Money Transfer   Western Union	🐴 🔹 🔊 🗉 🌧 🔹 <u>B</u> age + S	afety + T <u>o</u> ols + 🔞 + »
		<u> </u>
Track Money Transfer	Can we help?	
* indicates required field	Chat online or c free 24/7	all us toll
* Please enter Money Transfer Control Number (MTCN) below.		
Money Transfer Control Number (MTCN): 8527742553		
(MTCN): 8527742553		
Receiver's Country:* India		
Receiver's Country:* India		
3		
Amount* 19 Select a Currency V		
TRACK TRANSFER		
Don't know your MTCN or Phone Number?		
Home   About us   Contact us   Help   Consumer protection   Investor rela	ations   Careers   Western Union Foundation   Become an agent	
WESTERN UNION   About us   Contact us   Help   Consumer protection   Investor relation Intellectual property   Privacy policy   State licensing   File a complaint   @2001-2012 Western Union Holdings Inc. All Rights Reserved	Terms & conditions   Site map	
		~
Done	🛞 🚱 Internet	
😼 Start 🕥 🕤 (Trial version) HP Care 🚺 WESTERN UNION - N 🌈 Track a Mor	ney Transf	😰 🔇 🖲 🧐 🕲 8:09 PM

Session Three

On his third call, I again show "Roger" the fake "Western Union" page that tracks my transfer.

I changed the fake pages before his call so it would show him what I wanted him to believe this time.

Note again, that the URL again appears to be a valid Western Union URL.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

	http://status.westernunion.ca/track2.html	×	🗟 🗲 🗙 🔽 Bing	P
<u>E</u> dit ⊻ie•	w F <u>a</u> vorites <u>T</u> ools <u>H</u> elp			
Favorites	👍 🙋 Suggested Sites 👻 🙋 Free Hotmail 🌡	🕑 Web Slice Gallery 🝷		
Track a Mone	ey Transfer   Western Union		🏠 🔹 🔝 👘 🖃 🖶 🖓 Page 🔹 Safety 🕶	T <u>o</u> ols ▼ @▼
	W0-002 Pending			
	MTCN	: 8527742553		
	Transfer Status	: Pending		
	Transfer Availability	: August 26, 2013		
	Transfer Amount	: \$199.00		
	Transfer Currency	: Canadian Dollars		
	Sender	: Dave MacLaine		
	Sender's Office ID	: Money Mart #0648		
	Sender's Office Address	: 85 Prince Edward St		
	Sender's Office City	: Saint John		
		: Canada		
	Sender's Office Postal Code	: E2L 3S1		
	Receiver	: Tamanna Parveen		
	Receiver's Office ID	: Andhra Bank		
		: 101 A B T Road		
	-	: Kolkata		
		: India		
	Receiver's Office Postal Code	: 700090		
	Funds in the amount of \$199.00 CDN to	) Tamanna Parveen in Kolkata India will be available on		
		ary to complete the transfer between the new and old		
	network systems. Western Union and	its agents apologize for any inconvenience.		
Ple	ase Note: Transactions to certain destinatio	ns may take longer or be subject to additional restrictions.		

*Me:* "See, the transfer is working. But the girl said because you are on the old system, and we are on the new system, it will take a week because they have to transfer it manually."

*Me:* "Also, the girl at the Western Union office here said that because we have the new system, and India doesn't, you can't check the transfer from there. You can only check it from a computer in Canada."

Roger: "That is too long, let me check with my account manager."

I think "Roger" was expecting a more instant payment.

Note the fake page verifies the reason for the delay.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

📕 WESTERN UNION - Notepad		F	×
<u>File Edit Format View H</u> elp			
RECEIVERS FIRST NAMETAMANNA			^
RECEIVERS LAST NAMEPARVEEN			
COUNTRYINDIA			
CITYKOLKATA			
AMOUNT\$199			
PURPOSEPERSONAL			
10 MTCN NO			
MONEY MART #0648 85 Prince Edward St Saint John, NB E2L 3S1 506-636-8574			
emailhp.care24@yahoo.com			
Cust IDCAN 2023			
MONEYGRAM LOCATION:::::::			
SHOPPERS DRUG MART-CANADA POST			
57 LANSDOWNE AVE SAINT JOHN, NB E2K 2Z9 (506) 634-1774			
LAWTONS DRUGS-CANADA POST			
39 KING ST SAINT JOHN, NB E2L 4W3 (506) 634-1422			~
🛃 Start 🕥 🕞 (Trial version) HP Care 🕞 WESTERN UNION - N 🕞 WESTERN UNION - N 🌈 Track a Money Transf 😰 🤇	) 😧 🕲 8	:18 PM	

"Roger", or his "accounts manager" wants the money faster.

*Roger:* "One week is too long, too long. Tomorrow, you go to the Western Union office, and cancel the transfer. They will give you the money back. Then you go to send a Moneygram instead. You do this tomorrow, ok?"

Of course, I agree and tell "Roger" that I would take care of it in the morning. "Roger" makes me read the addresses to send a Moneygram from the note on my screen.

Next, we hang up and "Roger" does all the same things he did on the previous two calls. When he is done, he shuts down the computer.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca



### Session Four

Once again, I allow "Roger" in from remote. Once again, he is using the trial version of the remote access software.

After allowing "Roger" access, he gets additional help via a second remote connection. Apparently, he must think my computer is more than he is able to deal with by himself. Once again, I do my best not to laugh at him.



-06	limit the second	n	<b>v</b> 😣	Hang Bing	P
jie <u>E</u> dit	<u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp				
Favorites	👍 🙋 Suggested Sites 🝷 🙋 Free Hotmail	🖉 Web Slice Gallery 🔹			
🏉 Track a M	oney Transfer   Western Union			🏠 • 🔝 - 🖃 🖶 • Page •	Safety + Tools + 🔞+
WE	STERN		Canad	<b>da ▼ English ▼</b> Askaq	uestion Ask
moving	money for better			Customer Care Business Se	olutions Agent Services
					Register   Log In
	Track a Transfer				
	W0-067 CANCELLED				
	MTCN	: 8527742553			
	Transfer Status	: CANCELLED			
	Refund Availability	: August 28, 2013			
	Refund Amount	: \$199.00			
	Refund Currency	: Canadian Dollars			
	Sender	: Dave MacLaine			
	Sender's Office ID	: Money Mart #0648			
	Sender's Office Address	: 85 Prince Edward St			
	Sender's Office City	: Saint John			
	Sender's Office Country	: Canada			
	Sender's Office Postal Code	: E2L 3S1			
	MTCN 9537743552 in the amount of	\$199.00 CDN has been cancelled. If yo	u wish to re instate		
		nal availability date (August 26, 2013)			
	without additional delay within 24 ho		,ou muj uo oo		
	Refund will be available at the above	e sending office on August 28, 2013. Th	ie dolav je nocosearv		
		etwork infrastructure. Western Union a			
	apologize for any inconvenience.				
					>
Done		- 100		Internet	- • • • 100% •

Here we go back to my fake "Western Union" page, enter the information, and see that the transfer was indeed cancelled.

*Me:* "I cancelled the transfer, but the girl said because the transfer is between the new system and the old system, it will take a week for me to get my money back". *Roger:* "So you didn't send the Moneygram today?"

*Me:* "No, Western Union has all my money, I can't send payment until they give me my money back."

Roger: "Let me check with my accounts manager..."

I can tell by his voice that "Roger" is starting to get very frustrated. We hang up so I can pretend to go to bed, and "Roger" again works from remote.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

WESTERN	Canada My Profile Your Transactions Your last five approved transactions v displayed below. Use the "Send Again" feature to a	Sign Out My Profile Con	licks		
	Send Again Date Service	Transaction Ar		and Money Transfer Summary	
	Profile Overview     Manual Internation     Comment Version     Comment Version     Comment Version     Comment Version     Comment Version	Construction     C	I would like to use the following money transfer service           Available Services         Money is Available         Pey Win         What You Herd           Money in Minuse         Generally with minules at Minuse at Minuse at Minuse at Minuse Adams         Minuse Adams         The country where Minuse Adams           Money in Minuse         Minuse Adams         Minuse Adams         Minuse Adams         Minuse Adams           Amount I would like to send *         Minuse Adams         Minuse Adams         Minuse Adams         Minuse Adams           Vour and link for the brancadions CA 80 10.9         Your dily transaction limits that prevent you sending monourds grader than the limits immediate by local law.         Minuse Adams         Minus	Set d Amount (CAD):     400 00 C CAS Mittery Transfer Free:     200 C CAS 200 00 C CAS       Vesterna Union attrictly prohibits the use ondroir legal schulea:     200 00 C CAS 200 00 C CAS       WESTERNO: notion generative to stretchy on ondroir legal schulea:     Canada       Westerna Union® Money Transfer Service 1: Transfer Detals     2 Payment       • Indicates required field     1: Breview       • Indicates required field       I voudil like to use provitib Code:	Vie Transfer Status Contact Us   Rep Canada Consumer Services Tind a Contain Money Transfer Summary Send Amount (CAD) 400 00 CA S Chates Amount Honey Transfer Fee: 20 00 CA S Tota: 420.00 CA S
			_	The three-dight number of the back of the card number of the back of the back of the card number of the back of the back of the card number of the back of the card number of the back of the card number of the back of the bac	

Thinking I am not watching, "Roger" uses my browser to go to the real Western Union site. He starts to transfer money from a Mastercard belonging to someone in Alberta to someone in India.

It looks like they either recorded this information from a computer they installed spy software on when they were scamming them, or recorded it from their "payment site". Then they create a Western Union account in the victim's name, and without the victim's knowledge, so they can steal more money from them.

Just before "Roger" clicked on Continue to complete the transfer, I killed the power on the Virtual Machine. "Roger" called right away, and I told him we were having a thunder storm and the power went out. He agreed to call next day once the power returned.

I immediately took screen shots (including the name and address of the intended victim) to the city police, and asked them to contact the police in Alberta right away and inform the victim that their charge card was compromised.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

Windows XP Professional Setup

 Welcome to Setup.

 This portion of the Setup program prepares Microsoft(R)

 Windows(R) XP to run on your computer.

 • To set up Windows XP now, press ENTER.

 • To repair a Windows XP installation using Recovery Console, press R.

 • To quit Setup without installing Windows XP, press F3.

ENTER=Continue R=Repair F3=Quit

## Session Five

For our next session, I tell "Roger" my computer won't boot.

*Me:* "It says it wants SYSTEM DISC, I don't have a system disk. Did my computer break when the power went out last night?"

*Roger:* "Yes, your Windows is broken because of when the power went out. You need to go to where you got the computer and get two disks, a system disk and a driver disk. Then I will help you fix it."

I agree, and next day, "Roger" (with much help from his superiors) walks me through getting the computer to boot from the CD. This wasn't easy and took quite a while.

Me, trying really hard not to laugh: "I don't understand all this technical stuff".



While Windows is installing on my computer, "Roger" asks me a bunch of questions, things like where I work and other personal questions, all of which I answer not quite truthfully.

Because I am "one of his best customers" (after all, he seems to be spending most of his scammer career working on my computer), he is going to talk to his manager for me.

They are opening a new office, and need someone for "an exciting work at home opportunity". All I will need to do is collect payments, and receive my commission. Because I am such a good customer (even though he hasn't gotten a single penny from me yet), he will recommend my name to his manager. His manager will then call me directly to discuss my possible employment.

I haven't received a call from the manager yet, but I am pretty sure that when he does call, I will get the job, but there will be a "small fee to secure the position". That is how this type of scam usually works.

As Windows installs, every so often it requires input. Each time, "Roger" consults with his senior technician and then tells me what to do. Sometimes it takes me longer to accomplish what "Roger" asks, because (as I again tell him) "I don't understand all this technical stuff", and "I don't type very fast".

"Roger" continues to ask questions and chat.

*Me:* "Since we formatted my computer and are putting Windows back on, does this mean that all the viruses are gone now?"

*Roger:* "No no, the viruses hide in a secret place on the computer. I still need to fix it for you."

This time I cover the mouthpiece because I can't contain my laughter any longer.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

🖳 Device Manager	Network Setup Wizard
	Network Setup Wizard Ready to apply network settings The wizard will apply the following settings. This process may take a few minutes to complete and cannot be interrupted. Settings: Internet connection settings:
Keyobards     Keyobards	Connecting through another device or computer.          Network settings:         Computer description:         Computer name:         ANY-4CA19F6E31A         Workgroup name:         MSHOME
	< Back Net> Cancel

Now Windows is installed, but I tell "Roger" cannot get on the Internet. If I can't get on the Internet, "Roger" can't access my computer from remote.

"Roger" consults with his senior technician.

Roger: "You need to put in the drivers disk."

*Me:* "I only have one disk, the computer shop didn't give me any other disk."

*Roger:* "I told you to get TWO disks, not only ONE disk, you need the DRIVERS disk, TWO disks not one".

Me: "They only gave me one disk, and they didn't have another one."

This is another one of those times when I need to cover the mouthpiece on the phone so "Roger" can't hear me laughing.

"Roger" tries to get my Internet connection working. He gets me to open Device Manager and read anything with red or yellow next to it. I lied to him, and read "System Device, Video, and Ethernet" (the Ethernet driver was fine).

"Roger" then gets me to run the Internet connection wizard, and the network setup wizard. I wanted to yell at him "you stupid scammer, nothing you tell me to do is going to work without the Ethernet driver", but I held my tongue.

We gave up for the night, and I promised to get drivers the disk.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

## Between Sessions Five and Six

"Roger" called back asking if I got the drivers disc. I told him that even though I bought the computer used, I had it for less than thirty days, so it was still under warranty. I told him I would take it to the computer shop tomorrow, and they would put the drivers in for no charge.

Then "Roger" wanted to know if I sent the MoneyGram.

My wife had a good idea.

*Me:* "The girl at Moneygram said because of new anti-terrorist regulations in Canada, they need more information to send money out of Canada. They need the name and address of the accounts manager. The information has to come from a government issued ID card, and your accounts manager will need to show the card when he receives the money. If there are any mistakes, he won't be able to receive the payment."

*Roger:* "Let me check with my accounts manager..... Ok, I will give you the information from our other accounts manager from his ID card."

The name he gave matched the email address that he used to send the spy logs to, so the name and address I got from him is probably real. If it isn't his, it is for one of his accomplices.

I promised to send the MoneyGram after the long weekend, and he will call me back once the holiday is over.



"Roger" calls back on Tuesday as promised.

*Roger:* "How are you today? Did you have a good weekend? Did you get your computer back? Did you send the Moneygram?"

*Me*: "Yes, I got the computer back, they said it is all fixed, but I haven't hooked it up yet. I went to the Moneygram place, and they mailed you the payment."

Roger: "Did you get a reference number?"

*Me:* "No, they mailed it to the address you gave me, they said you don't need a reference number because they mailed it."

*Roger:* "How long did they say it would take to get here?"

Me: "I'm not sure, a week or two because it is overseas?"

Roger (sounding disappointed): "Oh, ok."

I told "Roger" that I had to rush back to work, and I had to work tomorrow night, so he should call me Thursday.



## Session Six



"Roger" called tonight. The last few nights I didn't answer (I had other things to do) but I decided if I wanted to keep him on the hook, I better take his call tonight.

*Roger:* "We have been worried about you, we have not been able to call you for several days."

*Me*: "Oh, at the Giant Tiger where I work, they are renovating the store, so I have to work many nights." *Roger*: "Oh, ok."

Last time we re-installed Windows from scratch, so "Roger" has to start over from the beginning tonight. He is still using a trial version of the remote access software, but now the name on the software is different. I am guessing that the previous trial has expired.

"Roger" asks me if I use the computer for online banking, because "under California law, I have to secure computers if they are used for online banking."

"Roger" is also very concerned about payment for "the service".

*Roger:* "What about payment, do you have the reference number for the money transfer? It has been forty seven days since we started the service, forty seven days."

*Me:* "No, there is no reference number, it was mailed."

*Roger:* "What exactly was mailed? Can you tell me exactly what was mailed? When will payment get here? Where did you send it?"

*Me:* "It was a Moneygram Money Order. It was mailed to the address you gave me, the girl said it will take one or two weeks, depending on the mail in India."

*Roger:* " Ok, ok, my bosses have been asking me about the payment, and I am worried they might fire me."

I try not to laugh too loudly while "Roger" begins work by installing Firefox.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

TeamViewer		🖗 Revealer Keylogger Free	X
Connection Extras Help Free license (non-commercial use only) - Dave - Any Nar Remote Control Meeting	re 💦 😔	Welcome to Revealer Keylogger Thank you for choosing our product.	English
Allow Remote Control Please tell your partner the following ID and password if you would like to allow remote control. Your ID 296 144 106 Password 9376 Enter a personal password to access this computer from anywhere. Personal Password Password	Control Remote Computer Please enter your partner's ID in order to control the remote computer. Partner ID Partner ID Remote control File transfer Connect to partner	By installing or using the product, you agree to its <u>User License Agreement</u> Install Now Customize	9
Ready to connect (secure connection)	Computers & Contacts >>		

Now "Roger" installs Team Viewer. It seems that every time he works on my computer, he needs two remote connections. I'm guessing he is just the "voice" while someone else actually accesses the computer.

Once again, "Roger" installs a key logging program on my computer. He doesn't say anything about this, he distracts me by talking about other things.

I play a loud wave file of a clap of thunder into the phone, and tell "Roger" we get thunderstorms all summer. I wanted an excuse in case I had to cut him off suddenly, if he tries to transfer money from someone else to India again.

"Roger" remembers that I don't have a PayPal account, so he is going to help me create one. But he has other things to talk about first.

He did "recommend my name" for the position with his company. All I have to do is receive payments on his company's behalf, deposit the cheques, and forward the money, minus my generous commission.

This is another scam. The cheques they send you look real, and when you deposit them, they go into your bank account. You send most of the money back to "Roger." The cheques take a long time to clear and two weeks later, the cheques bounce. The bank takes the money for the bad cheques out of your account, and you are that much poorer, while the scammer is that much richer.



#### Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

Google Accounts - Mozilla Firefox				
File Edit View History Bookmarks Tools Help				
C X 🏠 google.com https://ac	ccounts.google.com/SignUp?service=mail&cc	ontinue=htt 🏠 🔹 🚼 🗉 Google 🛛 🔎		
🖻 Most Visited 📄 Getting Started 🔝 Latest Headlines 📋 C	ustomize Links 📄 Free Hotmail 📄 Windo	ws Marketplace 📄 Windows Media 🛛 😕		
👂 Personal Account Sign Up - PayPal 🛛 🔯 Google	Accounts 🛛 😣 🕂	-		
Google		🐸 Personal Account Sign Up - PayPal - A	Aozilla Firefox	
0		Eile Edit View History Bookmarks Iools	; Help	
Create a	new Google Account	🔇 🔍 - C 🗙 🏠 🧬 PayPal,	Inc. (US) https://www.paypal.com/ca/cgi-bin/webscr?cmd=_f	ilow85E 🏠 👻 🚼 🔹 Google 🛛 🔎
Name		🔎 Most Visited 🗋 Getting Started 🔝 Latest He	eadlines 📋 Customize Links 📄 Free Hotmail 📄 Windows M	
		👂 Personal Account Sign Up - PayPal 🔞	M Inbox - maclainedave@gmail.com - Gmail 🖂 🕂	-
Dave	Maclaine	Enter your information		Secure 🔒 🔺
Choose you	ur username	Please fill in all fields.		
maclained	lave @gmail.com	Email address		
		You will use this to log in to PayPal		
Create a pa	assword	maclainedave@gmail.com		
	••	Choose a password		
Confirm yo	our password	•••••	Fair	
		Re-enter password	<ul> <li>Use 8-20 characters.</li> <li>Don't use your name or email address.</li> </ul>	
Done			Use a mix of uppercase and lowercase	
	e Accounts - M 😒 2 TeamViewer 8	First name	letters, numbers, and symbols.	
Guogi	e Accounts - M	1	<ul> <li>Make your password hard to guess - even for a family member or close friend.</li> </ul>	
		Middle name		
				9
		Last name		
			1	
		Transferring data from www.paypalobjects.com		
		Start (Trial version) HP Care	🕘 Personal Account Sig 😋 2 TeamViewer 8	- EN 👫 😯 😵 🧐 🏷 🚾 9:19 PM

Now it is time to set up my PayPal account.

Roger: "Ok, so what is your email address"

*Me:* "My wife does all that, she made me an email address, but I never used it." *Roger:* "Ok, we can make you a new email account."

"Roger" takes me to the gmail page and we create a new gmail account. He gets me to type in a password, and write it down, and tells me not to tell anyone. He doesn't ask me what it is, why should he? He already installed a key logger.

Then we create my PayPal account, using my new email address. Again, "Roger" gets me to type a secret password, while the key logger is still running silently in the background.

"Roger" tells me to enter my Social Insurance Number and cell phone numbers in the appropriate (but optional) boxes, I told him I didn't have a cell phone and I don't know my SIN.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

e <u>E</u> dit	View History	<u>B</u> ookmarks	<u>T</u> ools <u>H</u> e	nb							
$\langle \rangle \rangle$ -	C X	<u> </u>	ayPal, Inc. (	US) https://www.	paypal.com/	/ca/cgi-bin/websc	r?SESSION=bWi	☆ -	Soc	ogle	1
Most Visite	ed 📄 Getting S	tarted <u> </u> Lai	test Headline	es 📄 Customize L	inks 📄 Fre	ee Hotmail 📄 V	Vindows Marketp	olace 📄	Windows Me	edia	
Loading	J		XM	Inbox - maclaineda	ave@gmail.c	com - Gmail 🖂	÷				
				Sign Up	Log In   He	elp   Security a	and Protection			Sear	ch
-				0							
Pa	<i>Pal</i>										
Home	Personal	Business	s Devel	lopers 🛛 Whei	re To Use						
How Payl	Pal Works	Pay Online	Send Mo	ney Get Paid	Produc	ts & Services					
					Produc	ts & Services					
	Pal Works your PayF				Produc	ts & Services					
					Produc	cts & Services					
Sorry	your PayF	al sessio	on has tii	med out			out of PavPal	asase	curity preca	ution.	
	your PayF	al sessio	o <b>n has ti</b> i sn't been us	med out	ur system I	has logged you				ution.	
Sorry	your PayF Since your o Any unsave	<b>Pal sessio</b> computer has	o <b>n has til</b> sn't been us omplete trai	med out sed for a while, o nsaction you star	ur system I ted was di	has logged you iscarded. If you	came to this p	age from	m another		
Sorry	Since your of Any unsave website, ple	al sessio	o <b>n has til</b> sn't been us omplete trai o that site (d	med out sed for a while, o nsaction you star lon't use your bro	ur system rted was di owser's Ba	has logged you iscarded. If you ck button) and i	came to this p	age from	m another		
Sorry	Since your of Any unsave website, ple	al sessio	o <b>n has til</b> sn't been us omplete trai o that site (d	med out sed for a while, o nsaction you star	ur system rted was di owser's Ba	has logged you iscarded. If you ck button) and i	came to this p	age from	m another		
Sorry	Since your of Any unsave website, ple	al sessio	o <b>n has til</b> sn't been us omplete trai o that site (d	med out sed for a while, o nsaction you star lon't use your bro	ur system rted was di owser's Ba	has logged you iscarded. If you ck button) and i	came to this p	age from	m another		
Sorry	Since your of Any unsave website, ple	al sessio	o <b>n has til</b> sn't been us omplete trai o that site (d	med out sed for a while, o nsaction you star lon't use your bro	ur system rted was di owser's Ba	has logged you iscarded. If you ck button) and i	came to this p	age from	m another		
Sorry	Since your <b>PayF</b> Since your of Any unsave website, ple PayPal's we	Pal sessio computer has d data or inco ease return to obsite, enter y	on has til sn't been us omplete trai o that site (d your PayPal	med out sed for a while, o nsaction you star Iont use your bro I login informatio	ur system I ted was di owser's Ba n, and ther	has logged you iscarded. If you ck button) and i n click Log In.	came to this p restart your act	age fror tivity. If y	m another ou came fro		
Sorry	Since your <b>PayF</b> Since your of Any unsave website, ple PayPal's we	Pal sessio computer has d data or inco ease return to obsite, enter y	on has til soft been us omplete trai o that site (d your PayPal unts   Fees	med out sed for a while, o nsaction you star lon't use your bro	ur system I ted was di owser's Ba n, and ther and Protect	has logged you iscarded. If you ck button) and i n click Log In. <u>tion   Contact Us</u>	came to this p restart your act	age fror tivity. If y	m another ou came fro		
Sorry	Since your <b>PayF</b> Since your of Any unsave website, ple PayPal's we	Pal sessio computer has d data or inco ease return to obsite, enter y	on has til sn't been us omplete trai o that site (d your PayPal unts   Fees   Ma	med out sed for a while, o nsaction you star login informatio Privacy Security Sss Pay Qur Blog	ur system i ted was di wwser's Ba n, and ther <u>and Protect</u> Site Map	has logged you iscarded. If you ck button) and i n click Log In. ion   <u>Contact Us</u>   <u>Site Feedback</u>	came to this p restart your act   <u>Legal Agreeme</u> ®	age fror tivity. If y	m another ou came fro		
Sorry	Since your <b>PayF</b> Since your of Any unsave website, ple PayPal's we	Pal sessio computer has d data or inco ease return to obsite, enter y	on has til sn't been us omplete trai o that site (d your PayPal unts   Fees   Ma	med out sed for a while, o nsaction you star lon't use your bro login informatio <u>Privacy</u> <u>Security</u>	ur system i ted was di wwser's Ba n, and ther <u>and Protect</u> Site Map	has logged you iscarded. If you ck button) and i n click Log In. ion   <u>Contact Us</u>   <u>Site Feedback</u>	came to this p restart your act   <u>Legal Agreeme</u> ®	age fror tivity. If y	m another ou came fro		
Sorry	Since your O Any unsave website, ple PayPal's we	Pal sessio computer has d data or inco ease return to ebsite, enter y out Us   Accou	on has ti omplete trans that site (d your PayPal unts   <u>Fees</u>   <u>Mas</u> Co	med out sed for a while, o nsaction you star lon't use your bro login informatio Privacy Security sss Pay Our Blog pyright © 1999-207	ur system i ted was di wwser's Ba n, and ther <u>and Protect</u> Site Map	has logged you iscarded. If you ck button) and i n click Log In. ion   <u>Contact Us</u>   <u>Site Feedback</u>	came to this p restart your act   <u>Legal Agreeme</u> ®	age fror tivity. If y	m another ou came fro		
Sorry	Since your <b>PayF</b> Since your of Any unsave website, ple PayPal's we	Pal sessio computer has d data or inco ease return to ebsite, enter y out Us   Accou	on has ti omplete trans that site (d your PayPal unts   <u>Fees</u>   <u>Mas</u> Co	med out sed for a while, o nsaction you star lon't use your bro login informatio Privacy Security sss Pay Our Blog pyright © 1999-207	ur system i ted was di wwser's Ba n, and ther <u>and Protect</u> Site Map	has logged you iscarded. If you ck button) and i n click Log In. ion   <u>Contact Us</u>   <u>Site Feedback</u>	came to this p restart your act   <u>Legal Agreeme</u> ®	age fror tivity. If y	m another ou came fro		

I take my time as we fill out the form, and it takes long enough that it times out.

*Roger:* "It took too long, it is a secure site, the security times out."

Me: "Oh, I'm sorry, I don't type very fast."

*Roger:* "We will try again, this time you type in your password, and I will type everything else for you."

When it comes time to enter the banking info, I don't know what it is. "Roger" sounds disappointed.

*Roger:* "You don't know your bank account type or account number? You don't have your passbook or statement?"

*Me:* "No, my wife pays all the bills and does all that stuff."

*Roger:* "Oh, well when your wife gets home, you get the information and enter it here" (he points the mouse to the banking link on the PayPal screen).

I'm sure that if I did enter any real banking info into a PayPal account that "Roger" created for me (and for which he logged the password), money would quickly disappear from my bank account.



🖡 Untitled - Notepad	<b>    -</b>
File Edit Format View Help	4
are you there dave,,,pls hang up ia m calling you froomk a better lineok	<u>^</u> c
	1
	(
	1
	1
	v (
D Untitled - Notepad	ν
File Edit Format View Help	Long L

dave,today we are going to give you a short service.....

and tomorrow we will work for two hours and install the security license for lifetime

so you tell me whats the good time when i can call u back tomorrow??

ok i dont know if i work tomorrow nite but if im home 8 oclock is ok

#### we will try for sure

TeamViewer		
Connection Extras He Free license (non-commercial use Remote Control		
Legitimation Confirmation		
Do you know the p version of TeamVie		ent? This technician is using a free trial the person you are talking to.
		Trustworthy Decline (120)
computer from anywhere.     Personal     Password     Awaiting authentication		ect to partner Computers & Contacts >>
C:\WINDOWS\system32\cmd	.exe	- 🗆 ×
$\begin{array}{c} 1.4764.72068 \\ 0.91$	3,200 wowfax.dll 13,228 wowfax.dll 32,226 wopa.dbl 32,226 wopa.dbl 32,226 wopa.dbl 11,264 wpnpinst.exe 5,632 write.exe 13,968 ws2help.dll 13,824 ws2.22.dll 13,824 wscnffy.exe 156,648 wscnit.exe 156,648 wscnit.exe 1604,800 wscnit.exe 1604,800 wscnit.exe 1604,800 wscnit.exe 1604,800 wship.dll 14,336 wship.dll 14,336 wship.dll 14,351,168 wscnot.exe 11,264 WshNm.dll 14,354 wshorp.dll 14,454	

83 Prince Edward Street Saint John, N.B. E2L 3S1

#### Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

The phone connection isn't very good, "Roger" must be using VoIP from India, and frequently it breaks up. Finally, we can't hear each other at all, and "Roger" types a message for me to hang up and he will call me back.

The new connection isn't much better, so "Roger" types his messages in Notepad. He will "give me a short service" tonight, then tomorrow he will work for two hours and "install the security license for lifetime."

I type to "Roger" that I don't know if I have to work, but he can try at eight. We hang up so "I can go to bed" while "Roger" works from remote.

"Roger" sets Team Viewer so that it will automatically allow him remote access whenever he wants, without needing my permission.

Next he does all the same things he did before we formatted my computer. He did a defrag, ran the disk cleanup, check startup, etc.

Then he downloaded and ran "Software Pro Warranty Phase 1" which, the same as before, does nothing more than endlessly scroll a directory listing in a DOS window. This runs for about an hour, after which "Roger" shuts the computer down for the night.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

## Session Seven

During previous sessions, "Roger" has had an easy time working on my computer. Everything worked as he expected it to. For tonight's session, I decided to prepare things ahead of time to make things a bit more challenging for him.

I started by renaming some of the Windows commands. Notepad now opens Paint. Paint opens Calc. And so on. I did the same with some of the system control applets, so when he wants to view the system properties, he will get the accessibility wizard.

Then I added some custom entries to the hosts file, and prepared my firewall. When "Roger" tries to open Google, PayPal, Gmail, and a number of other sites, he gets a random page, a different one with each attempt.

So when "Roger" calls, he logs in from remote and I ask him about the problems the computer is having.

*Me:* "Oh good, I was waiting for your call, my wife says the computer is infected and all messed up, she can't get to PayPal or Ebay or Facebook or Banking and a bunch of other places, is it infected?"

*Roger:* "Yes, because you did not get the daily service it is a problem."

Me: "Ok, but since we have the lifetime service, you will fix it now?"

Roger: "Yes yes, we will fix it."

But no matter what he does, "Roger" cannot get to a number of pages, the wrong ones keep popping up.

Usually "Roger" sounds confident, but tonight he sounds a little less sure of himself.

We hang up so I can "watch TV" while "Roger" works from remote. But I think watching the virtual machine is going to be more entertaining than watching the TV tonight!



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca



"Roger" thinks I am watching TV while he works, and he will call me later.

He tries Google a number of times, and Paypal a number of times, and each time, the wrong page pops up. Each time he tries, he gets a different page.

He looks around the system, and does a few things to try to figure out what is happening. Nothing is working right for him.

Watching the screen, it is a good thing we hung up because I can't stop laughing. "Roger" has been trying to figure this out for about an hour, and it looks like he is stumped.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca



Now "Roger" installs the flash player. None of the pages he tried even use flash. I don't know why he thinks this will help, and, of course, it doesn't. Installing flash didn't fix anything at all, and the wrong web pages are still popping up.



"Roger" discovers that he is having more problems than just the wrong web pages popping up. When he tries to view "Add or remove programs", instead "Accessibility options" pops up. A number of programs open something different than what "Roger" expects. I burst out laughing, again.



When everything else fails, "Roger" tries the system restore.

The restore runs, setting the system configuration back to a time about a month ago.


Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

TeamViewer					
Connection Extras Help					
Free license (non-commercial use only) - Dave - Any Nar	ne 😽				
Remote Control Meeting					
Allow Remote Control	Control Remote Computer				
Please tell your partner the following ID and password if you would like to allow remote control.	Please enter your partner's ID in order to control the remote computer.				
Your ID 296 144 106	Partner ID				
Password 5560 9				_	
Enter a personal password to access this computer from anywhere.	े 🔂 Google Chrome Installe				
Personal Password	Installing Google Chrome				
h£			SETI@home ×		- 8
Ready to connect (secure connection)		+	→ × ♠ 🗋 setiathome.ssl.berkele	ey.edu	52
		I N	Londo your Llolo the Search f	I@home? is a scientific experiment that uses Internet-connected co or Extraterrestrial Intelligence (SETI). You can participate I n that downloads and analyzes radio telescope data.	omputers ir by running
		(	Click Here for More Information PARTICIPATE Download Get help	About SETI@home Message boards Your ac About Astropulse Questions & answers Prefere	ACCOUNT
		G	Tell a friend Donate Porting & optimizal	Science newsletters Profiles Certific Technical news User search tion Server status Teams	ate
			more	Science status Web sites & IRC <u>Sciences</u> Pictures & music Nore	
		G	Get started	News	
			software used by SETI@home. When prompted, enter the URL:	Android Beta Testers Needed We're beta testing the Android version of the SETI@horr application and we're looking for more testers to speed process. If you'd like to help, install the Android version through the Google Play Store or the Amazon App Store when asked to join a project enter	up the of BOINC a. Then
		Estal	http://setiathome.berkeley.edu	http://setiweb.ssi.berkeley.edu/beta as the project URL	
			and the second se	1@home - Google EN 🕱 🖲	0.2.0

After the system restore, "Roger" calls back and with his help I re-install TeamViewer, and "Roger" logs into my virtual machine. I'm sure he is hoping that the restore has fixed all his problems. Once he is connected, we hang up again while he works.

Now he installs Google Chrome. Last time, he told me never to use anything except Firefox, but I guess Chrome is the browser of the day today.

"Roger" types "www.google.com" in the address bar, but the SetiAtHome page pops up. I guess the system restore didn't help.

He tries Google a couple more times, and each time he lands on a different page.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca



This is where it becomes more obvious that "Roger" has help. My guess that the boiler room where he works has one or two slightly more technical people. This person (or persons), who "Roger" regularly consults, is probably responsible for writing the script, and directing the people who actually make the calls, and for handling anything unusual. And by now, my computer must appear unusual to them.

After snooping around the computer, "Roger" goes to the etc directory, and opens the lmhosts file. He is close, he wants the hosts file, not lmhosts, but the hosts file is hidden. "Roger" doesn't turn on viewing of hidden files, so all he sees is lmhosts. Since this file doesn't have anything unusual, he closes it and putters around the system some more. He comes back and opens the lmhosts several times, but it is the same each time.

He tries a few things, such as flushing the DNS cache, but nothing helps. Judging by the length of time between things "Roger" tries, I'm guessing he is looking up solutions on Google.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca



Since nothing he has tried so far has worked,

"Roger" transfers the trial version of AVG to my computer and installs it. He runs it but doesn't find any infections. I didn't think he would find any viruses, because I didn't put any in there for him to find.

The wrong web pages are still opening every time "Roger" tries to go to Google or many other sites. My wife in the next room hears me burst out laughing.



Now "Roger" tries clearing the Internet Are you sure you want Windows to delete your history of visited Web sites? Explorer cache and history. I shake my head, wondering why he thinks this should help when he was using Google Chrome.

He also deletes the temp files, checks the proxy settings, and does a few other things. "Roger" tries setting Internet Explorer to

	Invalid Proxy Server						
Э	8	The settings for the proxy server you've chosen to use are blank. This prevents access to the Internet. Do you want to turn off the proxy connection?					
)		Yes No Cancel					

automatically detect a proxy server, but this doesn't work. There is no proxy server on my network. Even if there were, I doubt that he would be able to configure Internet Explorer for it, it is obvious at this point the most of "Roger's" technical skill involves looking for solutions on Google, none of which he fully understands.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca



"Roger" tries Google, Bing, and PayPal several more times. Each time a random page pops up. He carefully goes through ALL the settings in the Internet Explorer control panel applet, and resets everything. He then resets all the settings on Chrome, and checks my IP address in a command prompt.

After a long wait, no doubt while he searches more on Google, "Roger" transfers a new hosts file to my computer, and overwrites my custom hidden one.



He immediately creates a restore point, in hope that he can quickly correct this problem if it occurs again.





Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca



After creating the restore point, "Roger" heads back to Google., but the wrong page comes up again! And again!! And again!!!

My sides are getting sore from all the laughing I have been doing during this session.



"Roger" checks the hosts file he just uploaded, and it is correct, the default Windows one.

The reason things went wonky on him again is because I simply took all the entries I had made in the hosts file, and pasted them into the nameserver on my firewall. Since the cause of the problem now isn't in the virtual machine, it is unlikely that "Roger" will be able to figure it out.

At this point, I wonder if scammers ever get nervous breakdowns, and if "Roger" is about to have one.

MCLEAN Professional Computer		83 Prince Edward Street Saint John, N.B. E2L 3S1 Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca		
🐸 Quick Heal Setup Downloader				
Quick Heal Setup Downloader	3			
Select the directory to download setup:				
C:\Documents and Settings\Dave\Desktop				
Download Information				
Status: Download in progress. Product name: Quick Heal Total Security 32-bit	Pause			
Download path: C:\Documents and Settings\Dave\Desktop\QHTSFT				
Statistics: 262.71 MB of 271.35 MB downloaded.	Turn off computer			
Transfer Rate: 2.20 MB/sec.				
Time Remaining: 3 sec. left				
Progress:		Quick Heal Total Security 2013 Settings Tools Reports Help •		
✓ Launch setup when download completes		Virus database 20 May 2013 Settings Tools Reports Help		
Open folder location when download completes		Scan Progress		
Options	Stand BL Turn Off	Performing full system scan		
Options	Stand Stand	Re: Eack to Dashboard		
		Scanning completed successfully. <b>O</b> NO virus found.		
		Please view reports for more details.		
		A		
		Skip Folder Skip File Eause Qose		

"Roger" now installs Quick Heal. It requires a reboot after installation, so he sets his remote access software to allow unattended remote login, and reboots the computer.

Once the system has rebooted and "Roger" has logged back in, he performs a scan with Quick Heal. Of course, just like the scan with AVG, nothing is found.

I am tempted to install a few viruses just for "Roger's" benefit, so there will be something for all his scans to find.

"Roger" proceeds to check everything he can think of, many of which could have any bearing on the problem he is having: Windows time settings, Windows firewall, free disk space, automatic updates, and more.

The wrong web pages still pop up when he tries Internet Explorer and Chrome again.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca



"Roger" also continues to experience other difficulties. When he tries to run the Services management applet, he gets the Local Security settings. When he tries to select Manage from the Computer context menu, he gets the Indexing Service.

I guess this sort of thing can happen if you rename some of the commands and applets before "Roger" calls. By this time, I'm too tired to laugh. "Roger" has been working for over three hours tonight.

After this, nothing happens on the screen for a while, and I want to go to bed, so I kill power to the virtual machine. "Roger" doesn't call when I do, and he didn't call the next night either, so I suspect he has had enough.

I wonder if I'll hear from him again?



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

# A Few Days After Session Seven

I haven't heard from "Roger" for several days, since he couldn't figure out why my computer wouldn't co-operate with him.

Here are a few random facts of interest about "Roger" and his attempted scam:

- A scammer makes a cold call and informs the victim that their computer is infected and needs to be cleaned. The scammer can do this from remote for a fee.
- The scammer works from a script, and sometimes can adlib if necessary, sometimes not.
- The scammer works in a "boiler room" under the direction of one or more scammers who are more technically knowledgeable, but still not real technicians.
- The payment site that they ask you to use may or may not capture your charge card information if you fall for the scam.
- The scammer will install spy software on your computer to gather information that may be used in the future. The information they want would include charge card and bank account numbers and passwords, PayPal login information, and any other information that may be useful to them.
- Once the scammer has banking/charge card/PayPal information, they will use it to steal money using a Western Union money transfer (which is NOT recoverable) or other money transfer service, so if you fall for the scam, you stand a good chance of losing more than just the initial payment.
- The scammer is not a single person who accesses your computer from remote, he is likely just the voice you hear. He will initiate remote access to your computer, and talk to you while he performs some simple tasks (many of which are useless but designed to make you think he is working), and then he will turn the remote connection over to someone else who has a bit more technical skill.
- The scammer runs additional scams, such as the fake cheque scam, that he may try to use on you.

Anyway, that is all for now. If "Roger" calls back, I will post an update.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

## Over A Week After Session Seven

I guess "Roger" hasn't given up yet.

The "accounts manager" called from India. Apparently, they still want payment. My wife said to call back at eight in the evening when I am home.

Sure enough, "Roger" calls back at about eight. I tell him I am busy, he will have to call back tomorrow.

He wants to talk for a moment about the payment, he is getting concerned. I promise to talk to the girl at the money place and have answers for him when he calls tomorrow "to finish the service" on my computer.

He suggests that I should get my money back and this time send it Western Union. I didn't remind him that I have already tried that (or, at least he thinks I did), and he told me to cancel it because it took too long.

I set things up again with my DNS and web servers to cause a bit of confusion on the virtual machine, so "Roger" should have an interesting time trying to fix things if he calls tonight.

If "Roger" figures it out and tries to manually set a DNS server in the network card properties, it won't help. My firewall is set to redirect all DNS queries from the virtual machine to my DNS server. No matter what "Roger" puts in for DNS settings, it will still use the DNS server I want.



💰 Disk Cleanup for (C:)

Disk Cleanup More Options

Downloaded Program Fil

🗹 🔒 Temporary Internet Files

Total amount of disk space you gain:

KebClient/Publisher Temporary Files

System Restore Automatic Updates

General Computer Name

🗹 🥑 Recycle Bin

🔽 🛋 Temporary files

Files to delete:

Description

System Properties

Run

Open:

File Edit

4 □

2 Q 1 🛔

 notepad

🦉 untitled - Paint

OK

View Image Colors Help

For Help, click Help Topics on the Help Men

You can use Disk Cleanup to free up to 49,052 KB of disk space on (C:).

Downloaded Program Files are ActiveX controls and Java applets downloaded automatically from the Internet when you view certain pages. They are temporarily stored in the Downloaded Program Files folder on your hard disk.

?×

0 KB 🔥

7.385 KB

517 KB

32 KB 🐱

49.020 KB

41 119 KB

View Files

Cancel

Remote

Advanced

<u>?</u>

~

Browse...

OK

Hardware

Professional Version 2002 Service Pack 3 Registered to: Dave

Any Name 76487-0EM-0047476-42340

Computer

Microsoft Windows XP

Intel(R) Core(TM) i7 CPU

950 @ 3.07GHz 3.07 GHz, 2.00 GB of RAM Physical Address Extension

OK Cancel

Cancel

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

System:

83 Prince Edward Street Saint John, N.B. E2L 3S1

Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

### Session Eight

The first thing "Roger" asked at the beginning of session eight was about the payment.

*Roger:* "My accounts department still has not got the payment. Can you send the payment again?"

*Me:* "I will ask the girl at the money transfer place about it tomorrow."

*Roger:* "I am getting in trouble with my accounts department, they are blaming me for no money."

*Me:* "Ok, I will go to the money transfer place again tomorrow."

Roger: "Ok ok".

"Roger" logs in from remote, and we hang up while he works. He does some of the same things again he did in the other sessions.

He does a disk cleanup, runs ATF Cleaner, and pokes around the system a bit, looks at settings and things, and in general doesn't accomplish much.

Then he runs "Software Pro Warranty" and the endless directory listing runs for a while.

He tries to open Notepad again, but as before, Paint comes up. Defrag doesn't work. Other programs don't work. The wrong things keep opening.

"Roger" isn't having much luck tonight.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca





Of course, the web still isn't working properly. My custom DNS and web server setup are still active. Just for fun, whenever "Roger" types in a web address, I quickly add it to my DNS server and redirect it to a random page. I can usually do this pretty quickly, so the page "Roger" wants never comes up.

Now he installs a couple of driver utilities. Since the web isn't working on my virtual machine, he has to download the utilities on his computer, and transfer them to my computer using the remote access software. Of course, running these utilities doesn't help.

Poor "Roger", nothing seems to be working for him, again.

At this point I almost feel sorry for him, but I remember that he is a thief that steals money from innocent people, and more often than not his victim is an elderly person who lacks the knowledge to spot the scam. So I think "Roger" deserves all the frustration I can give him.

After a while, "Roger" gives up for the night and shuts down the computer.



Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca



### Session Nine

"Roger" still hasn't given up. Usually, a scammer is done with the victim after a single session, but it appears that you can string them along for weeks if they think they have any chance of stealing your money.

"Roger" calls, asks again about payment, gets disappointed when it isn't there yet, and logs in from remote. He again complains that his accounts

department is blaming him for the lack of payment. I assure him he will get the payment soon, and we hang up so he can work from remote.

"Roger" does the same thing as before: he runs an endless directory listing from a batch file called "software pro warranty PHASE 1". I later looked at the batch file to see exactly what it does, and it is apparent that "Roger", or his technical supervisor, doesn't know a lot about batch files, and didn't look up how to write a simple FOR loop (or looked it up, but didn't understand it). Looking at the end of the file, it appears that there is a PHASE 2, if "Roger" ever gets that far, but so far he has never finished letting the 10,000+ lines of PHASE 1 run.

While the batch file runs, "Roger" tries to access several web sites, including the Western Union site. As before, the DNS and web servers on my network send him to the wrong sites.

He tries setting the home page in Google Chrome to the western Union page, but of course, that doesn't help either.

"Roger" pokes around the system for a bit longer, checks a few settings, and then gives up for the night. I don't know if he will call back again, or if he has finally given up.



MCLEAN MICRO Professional Computer Services Since 1993

Phone: 506-658-0486 Fax: 506-658-9652 Email: mclmicro@mcleanmicro.ca www.mcleanmicro.ca

# **Final Notes**

"Roger" left a voicemail last night, he has not been able to reach me. It has been about three months since he first called. I have learned what tactics this type of scammer uses to convince a victim to allow remote access to their computer, I have learned what they do to a victim's computer once they have access, and I have caused him hours of frustration.

So I am done with "Roger". If he calls, I will tell him I got the computer fixed elsewhere since we was unable to do so, and hang up on him.

Different groups of scammers may use different techniques and do different things to the victim's computer, so my virtual machine is ready for when the next scammer calls. But for now, I guess this is

# The End