

Whose problem is it? *ISP & Carrier Code of Conduct*

Craig Spiezle
Executive Director
Online Trust Alliance

SC World Congress
DATA SECURITY CONFERENCE AND EXPO
New York City 2010



OTA Mission

- **To drive a trusted online ecosystem by developing and advocating best practices that mitigate emerging threats to organizations and individuals**

SC World Congress
DATA SECURITY CONFERENCE AND EXPO
New York City 2010



OTA Overview

Initiatives

- Anti-malvertising
- Brand & Domain Protection
- Email Authentication
- Evolving Platforms & Devices
- Privacy & Public Policy
- Trust & Identity Frameworks

Values

- Best Practices & Guidelines
- Collaboration
- Education & Enablement
- Innovation
- Self-Regulation
- User Choice & Controls



Challenges

- An App for that...A hack for that...
- Blurred distinction *work, home & play*
- Portability of data & devices
- User is the weakest link
- Silent but deadly
 - Malvertising
 - Drive-bys
 - Zero day exploits

The Water Utility or Plumber?



Questions

- Are carriers mere conduits of data or do they need to protect consumers?
- Progress is being made on self-regulation, but is it enough?
- What is the role of the service provider
- Does the consumer have a shared responsibility?

ISP Practices

- Email Authentication
- EV SSL Certificates
- Account Verification / Password Management
- Discoverable & Clear Privacy Policies

- BOT / Malware Detection
- Drive EOL Browser Replacement
- Vulnerability detection
- Teachable Moments

Email Authentication

- Defense against spoofed & forged email
- Requires inbound and outbound



Detection & Remediation

Evolving Roles & Practices

- *Browser Upgrade*
- *Traffic Analysis*
- *PC Scanning*

U.S. studies Australia plan to force citizens to cure their PC infections

The government is reviewing an Australian program that will allow Internet-service providers to alert customers if their computers are taken over by hackers and could limit online access if people don't fix the problem.

By **LOLITA C. BALDOR**
The Associated Press

WASHINGTON — The government is reviewing an Australian program that will allow Internet-service providers to alert customers if their computers are taken over by hackers and could limit online access if people don't fix the problem.

Obama administration officials have met with industry leaders and experts to find ways to increase online safety while trying to balance securing the Internet and guarding people's privacy and civil liberties.

Experts and U.S. officials are interested in portions of the plan, set to go into effect in Australia in December. But any move toward Internet regulation or monitoring by the U.S. government or industry could trigger fierce opposition from the public.

Increase in hacking

The discussions come as private, corporate and government computers across the U.S. increasingly are being taken over and exploited by hackers and other computer criminals.

White House cybercoordinator Howard Schmidt said the U.S. is looking at a number of voluntary ways to help the public and small businesses better protect themselves online.

Possibilities include provisions in the Australia plan that enable customers to get warnings from their Internet providers if their computer gets taken over by hackers through a botnet.

Traffic Analysis

The screenshot shows a webpage from Qwest titled "QWEST'S CONSUMER PROTECTION PROGRAM" with the sub-header "THERE IS A POSSIBLE VIRUS ON THIS COMPUTER!". The page is designed as a wizard with several steps:

- STEP 1: Introduction** (highlighted)
- STEP 2: Remove Infections
- STEP 3: Removing the Virus
- STEP 4: Verifying Removal
- STEP 5: Restore Service

On the left, there is a "More Info" section with links for: Consumer Protection, Computer Security, Acceptable Use Policy, Privacy Policy, FAQs, and Technical Help. A "[Learn More]" link is also present at the bottom left.

The main content area explains that viruses can allow remote users to take control of a computer and steal personal information. It states that Qwest is concerned about the privacy of user information and would like to notify them of a possible virus. It offers to help find resources to address the issue and protect the computer. It also mentions that the Qwest Security Services team has received complaints about malicious traffic being sent from the user's Qwest account and has redirected their web traffic to the site to help remedy the problem.

At the bottom right, there are three radio button options:

- Remove Virus Now
- Remove Virus Later
- Already removed Virus

Qwest
Spirit of Service

More Info

- Consumer Protection
- Computer Security
- Accessibility: Use Policy
- Privacy Policy
- FAQs
- Internet Help

QWEST'S CONSUMER PROTECTION PROGRAM

Qwest constantly monitors its network for malicious Internet traffic. The network connections made from your Internet connection match commonly known patterns resulting from virus software. Qwest Internet Services Security is able to match the connections made from your IP address for a given time period to a Qwest account. When your account is associated with having a virus, your Internet connection is limited.

The Qwest Internet Security Services team has received complaints regarding malicious traffic originating from your account. Originating this type of traffic is a violation of your service agreement with Qwest and, as such, Qwest Internet Security Services is notifying you of this violation. Continued malicious traffic from this account may result in action including termination of your Internet services (termination of your Internet services may prevent your use of other services using the Internet, such as VoIP).

Qwest is committed to bring you the best possible Internet service. Although your current Internet session has been limited, these pages should help you find and remedy the virus that is interfering with your online experience. This limitation will be removed when you complete the instructions on the following pages and acknowledge you have done so.

Remember: Viruses can allow remote users to take control of your computer and steal your personal information.

Qwest
Spirit of Service

Virus Removal Steps

- STOP Introduction
- STEP 1: Account Verification
- STEP 2: Removing the Virus
- STEP 3: Working Removal
- STEP 4: Restore Service

More Info

- Consumer Protection
- Computer Security
- Accessibility: Use Policy
- Privacy Policy
- FAQs
- Internet Help

QWEST'S CONSUMER PROTECTION PROGRAM

PLEASE VERIFY YOUR ACCOUNT INFORMATION:

Qwest has identified your account as:

Qwest.net User ID:	csrig1234 *
Reported Virus:	Conficker
Virus Description:	The Conficker Worm, (aka 'Downadup'), is malicious software that automatically spreads by exploiting software vulnerabilities on unpatched computers, and attempts to infect other computers. Computers infected with this problem may be subject to any of the following: <ul style="list-style-type: none"> Identity theft, including theft of password, bank account, and credit card information stored or entered on the computer Remotely view, change, or delete information stored on your computer Performing or participating in attacks on other Internet users or sites Remote installation of unwanted software on your computer Reduced Internet and computer performance Disabling or removing antivirus or computer security software

Qwest
Best of Service

Virus Removal Steps

- STEP 1: Introduction
- STEP 2: Account Verification
- STEP 3: Removing the Virus**
- STEP 4: Verifying Removal
- STEP 5: Restoring Services

More Info

- Consumer Protection
- Computer Security
- Acceptable Use Policy
- Privacy Policy
- FAQs
- Internet Help

QWEST'S CONSUMER PROTECTION PROGRAM
REMOVING THE VIRUS

Special Advisory: Conficker can disable security software.

The following tool specifically removes most variants of the Conficker virus and should be run first. After running this tool, you should update your Anti-Virus (AV) software and definitions and run a complete scan of your computer.

[Microsoft Malicious Software Removal Tool](#)

Below are some steps you can take to improve your computer security.

- Review our recommended [good security practices](#).
- If you have Windows XP Home Edition, Windows XP Professional, Windows 2000 Professional, Windows Server 2003, or Windows 2000 Server and either Microsoft Internet Explorer 6.0, or MSN 9.0, the [Windows Live Safety Center](#) can help you.
- Open your AV software and update the virus definitions according to your AV software's instructions. You can lookup information about your AV software if it is from one of the vendors below:
 - Trend Micro
 - Avast

Qwest
Best of Service

Virus Removal Steps

- STEP 1: Introduction
- STEP 2: Account Verification
- STEP 3: Removing the Virus
- STEP 4: Acknowledgement of Virus Removal**
- STEP 5: Restoring Services

More Info

- Consumer Protection
- Computer Security
- Acceptable Use Policy
- Privacy Policy
- FAQs
- Internet Help

QWEST'S CONSUMER PROTECTION PROGRAM
ACKNOWLEDGEMENT OF VIRUS REMOVAL

In order to reestablish your Internet connection, please acknowledge that you have removed the virus by checking the box and clicking continue:

I Have Removed the Virus

[← BACK](#) [CONTINUE →](#)

Traffic Analysis

comcast.net Security

Security News | Get Protected | Get Smart | Get Help

Constant Guard Center

You have been directed to this page by the Comcast "Service Notice" because we believe it is very likely that one or more of the computers in your household have been infected with a Bot or malicious software, known as Malware. Not only may this critical infection cause your computer to run slowly, but it could increase your risk of identity theft and use your computer to send spam.

To assist in the removal of the Bot or Malware, you can choose the do-it-yourself option or, for a fee, get professional assistance. The professional assistance information can be found below.

Do-It-Yourself Option

To get started, please select your Operating System (OS):

Windows

FAQs

- What is Constant Guard?
- What is a "Service Notice"?
- How did Comcast determine that I may have a bot?
- Did I get an infection from the page I was browsing?
- How could I have gotten a bot?
- Why am I receiving multiple "Service Notices"?
- What is a Bot?
- What is the difference between Malware and Virus?

[More FAQs...](#)

Comcast Recommendations

- Comcast Toolbar (Anti-Fishing, Anti-Spyware)

Browser Upgrade

Information Regarding Web Browsers - Windows Internet Explorer

http://www.browserchoice.eu/DownloadChoice.aspx.html

Select your web browser(s)

<p>Google Chrome A fast new browser. Made for everyone.</p> <p>Install</p> <p>Tell me more</p>	<p>Safari Safari for Windows from Apple, the world's most innovative browser.</p> <p>Install</p> <p>Tell me more</p>	<p>Mozilla Firefox Your online security is Firefox's top priority. Firefox is free, and made to help you get the most out of the web.</p> <p>Install</p> <p>Tell me more</p>	<p>Internet Explorer Internet Explorer is the world's most widely used browser, designed by Microsoft with you in mind.</p> <p>Install</p> <p>Tell me more</p>	<p>Opera browser The powerful and easy-to-use Web browser. Try the only browser with Opera Turbo technology, and speed up your Internet connection.</p> <p>Install</p> <p>Tell me more</p>
---	---	---	---	---

Select Later

[Further information](#), [Terms of use](#) and [Privacy statement](#).

PC Scanning

Personal Software Inspector (PSI) 2.0 BETA 96% Secunia System Score

Dashboard

Quick Summary

Secunia Community Profile: Unregistered user

Last Scan: 4 Nov 2010, 00:00

Secunia CVE Mitigation: 0 CVEs detected

Auto-Updates: 0 security patches installed
Last install: 12 Oct 2010, 00:00

Auto-Update History: [Table with columns: Program Name, Version, Status]

Your PC: **Current State: 96%** **Low Risk**

Secunia System Score: 96%

State of Progress: **Tracked: 7** **Out-of-date: 1** **Not tracked: 22**

Comparison to New York, United States: **96%**

User Type: **Average user with Secunia PSI: +2%** **Average user without Secunia PSI: -42%**

Development in your Secunia System Score for the past weeks: [Bar chart showing scores of 96% over 5 weeks]

Security patches for your programs during the past months: [Line graph showing patch activity]

SC World Congress
DATA SECURITY CONFERENCE AND EXPO
New York City 2010



Personal Software Inspector (PSI) 2.0 BETA 99% Secunia System Score

Scan Your Computer

The scan of your PC completed successfully. A quick summary of the scan is available below. For more details, please click the "View Scan Results" button.

Secunia System Score: **99%**

Programs found: **8** Tracked programs **1** Out-of-date programs **19** Not tracked programs

Total

View Dashboard | View Scan Results

SC World Congress
DATA SECURITY CONFERENCE AND EXPO
New York City 2010



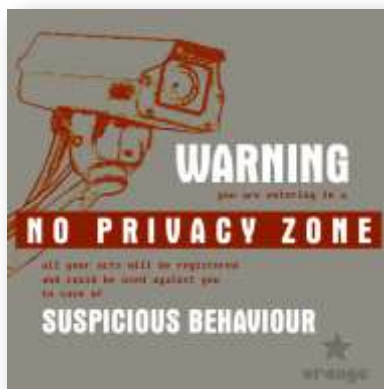
Considerations & Challenges

- Cost
- Privacy
- False Positives
- Consumer Churn
- Cart Abandonment

SC World Congress
DATA SECURITY CONFERENCE AND EXPO
New York City 2010




Re-Thinking Expectations




SC World Congress
DATA SECURITY CONFERENCE AND EXPO
New York City 2010






NOT MY JOB

SC World Congress
DATA SECURITY CONFERENCE AND EXPO
New York City 2010



Who's Job is it?



© Original Artist
Reproduction rights obtainable from
www.cartoonstock.com

SC World Congress
DATA SECURITY CONFERENCE AND EXPO
New York City 2010



It is all of our jobs

- Security, Privacy & Data Stewardship
- Business, Industry, Government
- **And Consumers**



SC World Congress
DATA SECURITY CONFERENCE AND EXPO
New York City 2010



ISP Ratings ?



SC World Congress
DATA SECURITY CONFERENCE AND EXPO
New York City 2010



Key to Innovation - Balance

- Consumer Choice
- Collaboration
- Security
- Privacy
- Self-Regulation



Resources

- OTA Anti-Malvertising
<https://otalliance.org/malvertising.html>
- Email Authentication
<https://otalliance.org/resources/authentication/index.html>
- Resources & Solutions
<https://otalliance.org/resources/index.html>
- Membership <https://otalliance.org/join.html>
- Questions staff@otalliance.org

Thank You



SC World Congress
DATA SECURITY CONFERENCE AND EXPO
New York City 2010

