



To: Representatives of the Financial Services Roundtable, GAC, Public Affairs Council, Research Council, All Staff

## **Fast Facts: Malware Risks & Mitigation**

**FACT:** *Malware* is malicious computer code with which cyber criminals try to infect a computer system, compromise its security controls, and steal information.

**FACT:** In 2010, reports of [malware infection grew to 64.3%](#) (from 50% in 2009) among U.S. corporations, government agencies, financial institutions, educational institutions, medical institutions and other organizations.

**FACT:** In April 2011, [one in every 168 emails contained malware](#), rising from one in every 208 emails in March of 2011.

**FACT:** [Financial services firms were the primary targets](#) in 33% of 2009 and 22% of 2010 cases, making them the most targeted sector in 2009, though in 2010 they were surpassed by hospitality and retail.

**FACT:** Financial institutions protect against malware through security controls such as ongoing, threat-based software patching programs; strong software change control processes; system and traffic log monitoring; firewalls; and incident reporting and response plans.

**FACT:** This week, BITS released a [“Malware Risks and Mitigation Report”](#) to assist financial institutions and related industry stakeholders to identify and address malware risks at the enterprise level and to collaborate with others to address malware more broadly.

**FACT:** Additionally, ITAC, the Identity Theft Assistance Center, led by [Anne Wallace](#) at the Roundtable, [recently conducted a "radio tour"](#) to alert consumers to the fraud and identity theft risks associated with malware.

*BITS is the technology policy division of The Financial Services Roundtable. BITS addresses issues at the intersection of financial services, technology and public policy, where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services.*

As always, please do not hesitate to contact Abby McCloskey, Director of Research at the Financial Services Roundtable, at [Abby@fsround.org](mailto:Abby@fsround.org), Scott Talbott, Senior Vice President of Government Affairs, at [Scott@fsround.org](mailto:Scott@fsround.org), or Greg Rattray, BITS SVP of Security, [Greg@fsround.org](mailto:Greg@fsround.org) or 202-589-2442.



## **10 Ways to Protect Yourself From Computer Fraud**

1. Install and keep anti-virus/anti-spyware software updated on your computer and phone.
2. Only do business with trusted firms.
3. Don't store personal or business information, passwords or account numbers online.
4. Use a secure web connection – look for https:// in the browser – before conducting business online.
5. Use a firewall to protect your PC.
6. Turn on automatic patching of your operating system and regularly update you software applications.
7. Secure your wireless router by employing a firewall, using strong passwords and enabling wireless encryption (such as WPA or WPA2).
8. Create account passwords that use 8+ characters in a combination of letters, numbers, upper and lowercase and symbols.
9. When you bank online, remain at your computer until the transaction is completed and sign off completely when finished.
10. Don't provide personal information online unless you know where it is going and what it will be used for. Review privacy policies and website certificates.

**For more information about consumer protection, please contact Greg Rattray, BITS SVP of Security, [Greg@fsround.org](mailto:Greg@fsround.org) or 202-589-2442.**