

**The  
INTERNET  
HIGHWAY  
CODE**

**STAYING SAFE ONLINE**

**Alan Calder**

## **About the author**

Alan Calder is a businessman who, during many years of running companies of all sizes in both the public and private sectors, has grappled with geek-speak around computers and information security. He believes that information security is as fundamental to everyday sensible behaviour as household security.

The truth is that it's the geeks who are advancing the capability of modern computing and, therefore, it is essential that everyone else understand what is going on and how, simply and pragmatically, to cope.

Alan is a founder director of IT Governance Ltd ([www.itgovernance.co.uk](http://www.itgovernance.co.uk)), a consultancy firm that helps company boards tackle IT governance, information security and risk management.

The company operates a website ([www.itgovernancesales.co.uk](http://www.itgovernancesales.co.uk)) through which it provides a range of information security tools, including pre-written policy and procedure templates and guidance manuals and tools for BS7799/ISO17799 implementations. It also provides a range of tools for corporate wireless security projects.

### **Other titles:**

[“IT Governance: a Manager’s Guide to Data Security and BS7799/ISO17799”](#). Third edition published June 2005.

[“IT Governance: Guidelines for Directors”](#) (April 2005)

[NON-Geek Guide to wireless Security](#)

“ABCs of Information Security” is due out later in 2005.

“Corporate Governance: a Practical Guide” is due out in late 2005.

## CONTENTS

<b>Preface</b>	1
The 10 Rules of the Internet Highway Code	1
<b>Introduction</b>	3
Threats and Risks	4
Looking ahead	6
Implementation Guidance	7
Identify your operating system	7
<b>1 Safeguard your computer</b>	9
<b>2 Use strong passwords and a screensaver</b>	11
<b>3 Update and patch your operating system</b>	14
<b>4 Have an up-to-date firewall</b>	17
<b>5 Have up-to-date anti-virus software</b>	19
<b>6 Act anti-spam</b>	21
<b>7 Use up-to-date anti-spyware/adware tools</b>	24
<b>8 Be sensible – don't take unnecessary risks</b>	27
Be alert – pay attention – be sensible	27
E-cards	28
File sharing	28
Identity theft	29
Internet cafes and other public computers	30
Online auctions	31
Online charities	31
Online payment services	32
Online recruitment services	32
Online shopping	32
PDA's and mobile phones	34
Phishing	34
Safe surfing for children	35

	Scams, frauds, 419s	36
	Spoofed e-mail addresses and Websites	36
9	<b>Back it up</b>	38
10	<b>Fix problems as soon as they arise</b>	40
	<b>Glossary</b>	42
	<b>Further reading</b>	55
	<b>Useful websites</b>	56

## PREFACE

When you go away, leaving your house unoccupied, do you lock the front door? And do you only lock the front door, leaving lots of windows open, or do you also make sure that at least your ground floor windows are all shut and locked? What about the back door? Would you bother with an alarm? Why?

And if you were to park your car in a dodgy area, would you lock the doors before you walked away from it? Would you bother with a car alarm, or a steering wheel lock? Are there some areas where you might even want someone to stand guard over your car while you were gone?

And if you went into a shop that was advertising huge discounts on incredibly expensive sun-drenched holidays at a five star hotel in the Caribbean, and there was no till, just a man in dark glasses who wanted payment in cash - in full - today - in exchange for which he was promising to send you your tickets in a month's time, would you be likely to hand over any money at all?

Yes, the physical, analogue world has a number of fraudsters, charlatans and thieves who are keen to steal your money and your goods, and you are used to taking precautions against them. It's no different on the Internet - no more safe, and no less. That's important: the Internet is not less safe than the physical world. If you don't take appropriate precautions, you can expect - sooner or later - to pay the price. On the Internet, the bad guys are just a mouse click away - and most of the interesting and cool things to do are also not yet very secure. You can use the Internet perfectly safely, as long as you remember to apply basic common sense, and take the basic precautions - by following the **Internet Highway Code**.

### **THE 10 RULES OF THE INTERNET HIGHWAY CODE:**

1. Safeguard your computer

2. Use strong passwords and a screensaver
3. Update and patch your operating system
4. Have an up-to-date firewall
5. Have up-to-date anti-virus software
6. Act anti-spam
7. Use up-to-date anti-spyware/adware tools
8. Be sensible – don't take unnecessary risks
9. Back it up
10. Fix problems as soon as they arise

## **INTRODUCTION**

We live in an analogue world and, increasingly, work, play and do business in a digital one. Our assets, the things we own in either world and that are valuable to us, are also attractive to others. As we've extended our field of activity into the digital World Wide Web (or Internet), as we've developed new technologies and acquired new skills, so we've been followed by all those anti-social elements who plagued us in the analogue one.

Over the centuries, we've become accustomed (particularly in the first world) to taking appropriate precautions around our analogue assets, health and security. We know how to secure homes, offices and cars. We know what precautions to take while walking, shopping or doing business. We know which neighbourhoods to stay out of. We teach our children what to do, and we have well-developed police and justice systems that deal (to one extent or another) with miscreants.

Although the police and justice systems are still coming to grips with the digital world, the miscreants – criminals (of all sorts: organized, white collar and occasional), malefactors, spies and other undesirables – have already successfully adapted their modus operandi to cyberspace. Of course, that doesn't mean that they've deserted the analogue world, they've just extended their

sphere of operations to the digital one. We've therefore got to get as good at dealing with the cyber threats and risks as we already are at dealing with the analogue ones.

In the same way that the average individual can understand the rules for maintaining and driving a motor car without having to be an auto-mechanic, so any computer user can understand how to be safe online, without needing to be a computer expert. Just as you would be hard-pushed to help a medical specialist diagnose and cure an illness, without first having a good idea of what it takes to stay healthy, or what disease feels like, so it would be difficult to ensure that your home network or personal computer was adequately secured – or even to call in appropriate outside help - without some grasp of the basic threats.