

A close-up, vertical shot of a computer keyboard. The 'Enter' key is the central focus, with the word 'Enter' printed in white on its grey surface. The surrounding keys are blurred, and the lighting is dramatic, highlighting the texture of the key.

**McAfee**

**Enter**

**McAfee**

# Mind Games Report

How cybercriminals are exploiting psychological vulnerabilities to gain your money and information

**Organised criminals are constantly looking for the next new opportunity to exploit PC users for their own gains. The growing ingenuity of cybercriminals is proving a serious challenge for consumers, businesses and law enforcement organisations.**

A far cry from simple mass attacks, cybercriminals are increasingly combining stealth code-writing with psychological cunning through mind games to trick PC users into giving up personal information and money.

They are taking advantage of the temptation for us to suspend disbelief online. Many of us slip into the trap of believing that online activity is safer than real life and that the real world risks do not happen in the virtual universe.

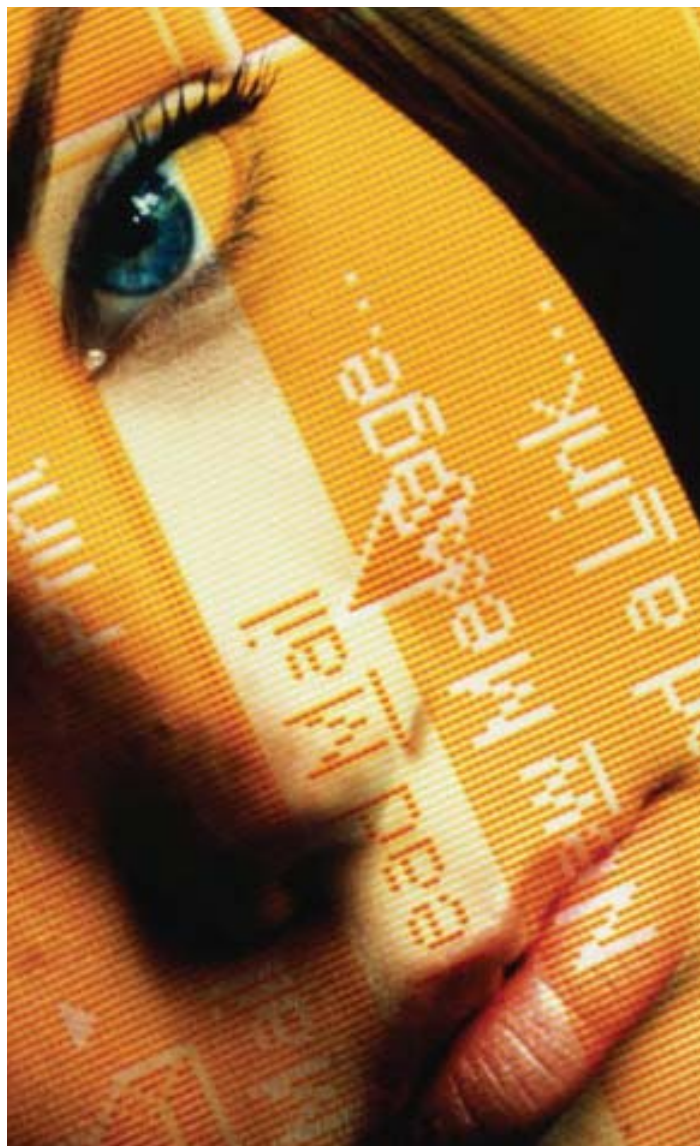
These 21st Century grifters are drawn in by the Internet's anonymity and global reach. They are using traditional offline scams and adapting them to this low risk, high return environment.

According to the European Commission, online scams are now the fastest growing category of fraud in Europe.

The McAfee Mind Games Report looks at the latest trends and suggests how to fight back against the cyber-mind manipulators.

McAfee has worked with a leading forensic psychologist, Professor Clive Hollin, based at the University of Leicester in the UK, to analyse why we fall for online scams identified by McAfee's global Avert Labs.

**Greg Day, Security Analyst at McAfee.**



**Mind Games – plural noun:** Often, mind game, psychological manipulation or strategy, used esp. to gain advantage or to intimidate.

“A Mind Game can be seen as an interaction, typically conducted through an email or website, between the individual who designs and initiates the Mind Game and their intended target. In this respect the interaction is dynamic in nature: the designer has the clear (fraudulent) intention of setting up the Game to engage an exchange with the target, while deceiving them of the real purpose of the interaction, in order to achieve some type of gain.”

Professor Clive Hollin

## CONTENTS

- 01 INTRODUCTION
- 02 MIND GAMES – A GROWING THREAT
- 03 HOW CYBERCRIMINALS ARE MANIPULATING THE WAY WE PROCESS INFORMATION
- 04 WHO'S AT RISK FROM CYBER-MIND MANIPULATION?
- 05 THE TACTICS OF DECEPTION
- 08 MIND GAMES – A CONSTANTLY EVOLVING THREAT
- 09 AVOIDING CYBER-MANIPULATION
- 10 METHODOLOGY
  - ABOUT MCAFFEE AVERT LABS
  - ABOUT PROFESSOR CLIVE HOLLIN

Cybercriminals are employing increasingly devious means to manipulate people into handing over money and personal information.

By understanding the psychology of how we process information in the way we do, cybercriminals are creating increasingly sophisticated email scams which manipulate our deepest psychological vulnerabilities.

The example on the right is one of a growing number of email scams which use psychology to manipulate our behaviour. In this instance the scam preys on our deep-seated fear of being hauled into court.

The subject line in an email that hit thousands of inboxes around the world read “legal action against you”. In flawless legalese, the message warned recipients that they recently sent an unsolicited fax to the sender’s office. Citing US civil code, its prohibition on sending junk faxes and an actual \$11 million settlement by restaurant chain Hooters, the missive threatens a lawsuit over the alleged junk fax. “If you don’t pay me \$500 by the deadline for payment, I intend to sue you for violating the Telephone Consumer Protection Act,” it reads. “If you force me to sue, I will not settle for less \$1,000”. Details of the alleged lawsuit are contained in the email’s attached document.



In today’s litigious – and digital – society, being notified of legal action via email might not seem too unusual right? Wrong. The attachment – labelled lawsuit.exe – contained a new variant of a computer worm. When worried victims opened the attachment, malicious code embedded in its text downloaded onto their PCs and swiftly harvested the victims’ email addresses to send malicious code disguised as subjects like ‘Paris Hilton sex video’ to their friends and colleagues.



## HOW CYBERCRIMINALS ARE MANIPULATING THE WAY WE PROCESS INFORMATION ✕

Psychological processes control human functions such as behaviour, perception and reasoning – all the different things the brain controls. By understanding how our minds process information and what inspires us to act on it, our actions can be manipulated online just as they are offline.

Communication over the Internet typically comes in the form of the written word (rather than verbal) – although this may well change as technology advances – along with the various cues (website links, popups, email addresses, etc.) associated with web pages.

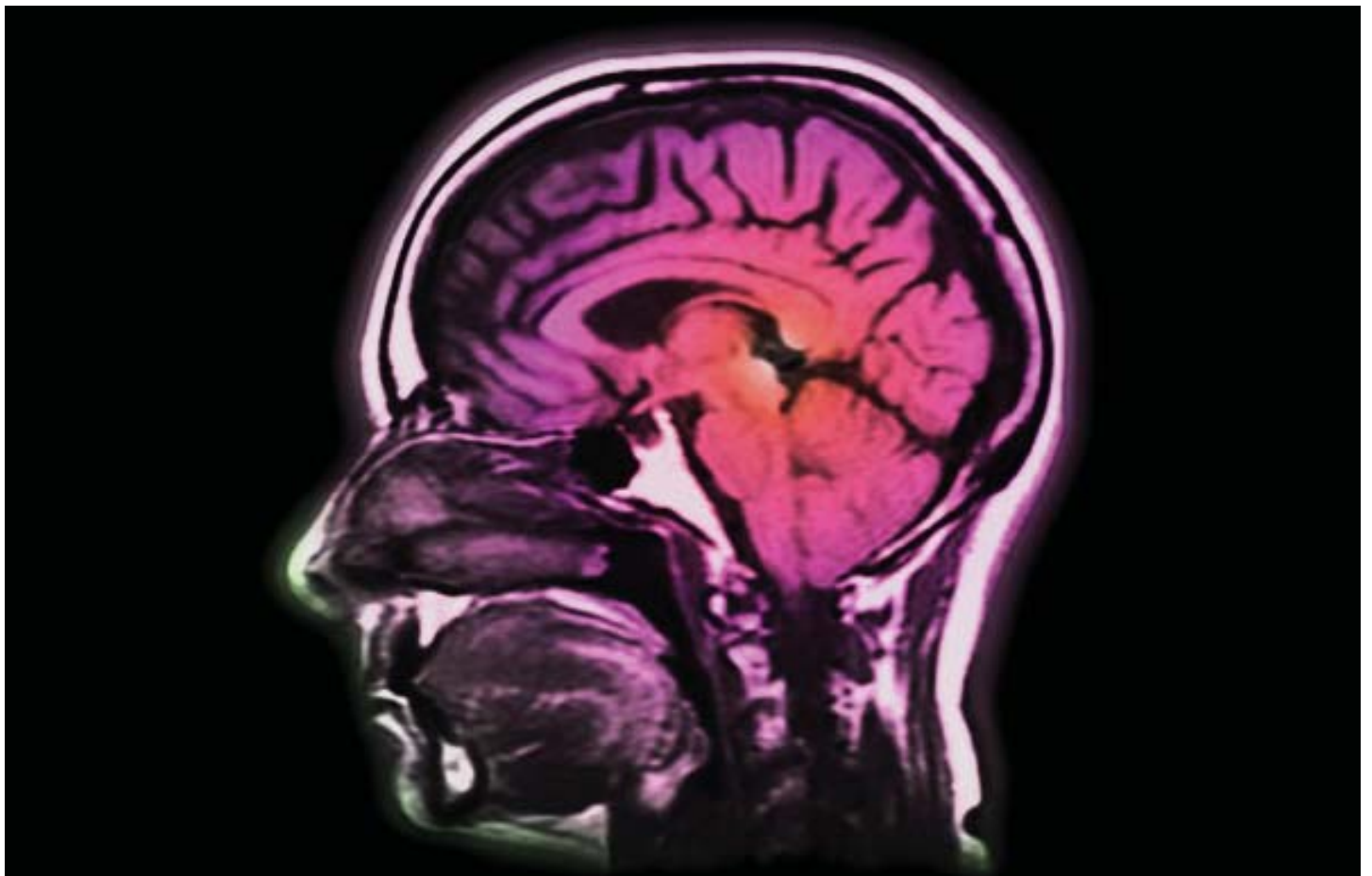
When processing information online, our first step is to perceive and process the 'cues' or prompts we receive such as website links, popups, email addresses embedded in the message on the screen.

When we read a web page we are taking part in a form of social interaction as we would do in the real world but on the web the flow is one way (web page to reader). And unlike most social interactions, one "person" (communicating via the web page) now holds the balance of power.

Cybercriminals are exploiting these social interactions online using a variety of different techniques including 'phishing' – where cybercriminals try to acquire sensitive information by impersonating a trustworthy entity via email. Another example is 'gimmes' – where fraudsters deliver attachments loaded with malware and encourage us to open them by appealing to our sense of curiosity or desire for gain.

"Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face to face with the victim."

Wikipedia





## WHO'S AT RISK FROM CYBER-MIND MANIPULATION?

Contrary to popular belief, it is not simply the inexperienced that fall victim to online scams. In fact, the volume of online scams indicates cybercriminals are successful in ensnaring all sorts of users.

One aspect of human behaviour which is being manipulated by cybercriminals is that of 'suggestibility' – or how susceptible we are to social communications in certain situations.

“Given the right conditions in terms of the persuasiveness of the communication and the critical combination of situational and personal factors most people may be vulnerable to misleading information. This point is true both for experienced and inexperienced computer users: while naivety may be a partial explanation, even sophisticated users can be deceived and become suggestible to misleading messages.”

Professor Clive Hollin

When we are in a 'suggestible' state, we receive, interpret, and evaluate the information in a biased manner as intended by the fraudsters. We discount any logic and suspend our critical, problem-solving abilities.

### HERE ARE JUST A FEW 'TYPES' THAT CAN PROVE VULNERABLE:

#### NEWCOMERS TO THE WEB

Newcomers or inexperienced web users are likely to be unaware of basic online dangers and can be easily drawn in. A trusting attitude towards emails received can leave people open to the vital trigger of believing that emails are from a legitimate source.

#### BARGAIN HUNTERS

Those looking for bargains or those who act on what they see as easy gains or excitement are at risk from the temptation offered by the promised, but never delivered, rewards.

#### TECH-FRIENDS

Technology and Internet penetration is at an all-time high and the familiarity of this environment can breed over-confidence. With online task-based and entertainment activities becoming an essential part of daily life for so many, there can be a tendency to grow blazé about the associated risks.

#### SEEKERS

Changes in personal circumstances can prompt different psychological triggers which can leave people more open to cyber-manipulation. For example a recently single user is far more likely to be motivated to interact with a dating scam, just as a recently unemployed user would be more likely to respond to a 'working from home' scam.

“The typical victims of crime are the vulnerable, the naïve, and the risk-takers in society. The vulnerable become victims because their vulnerability, either personal or being in the wrong place at the wrong time, is recognised and exploited by perpetrators; the naïve because they are easily drawn in; and the risk-takers because they act on what they see offered as easy gains or excitement.”

Professor Clive Hollin



Yet even accounting for the ways in which people may be pre-disposed to fall for certain types of tricks, scammers realise that most users will be sceptical.

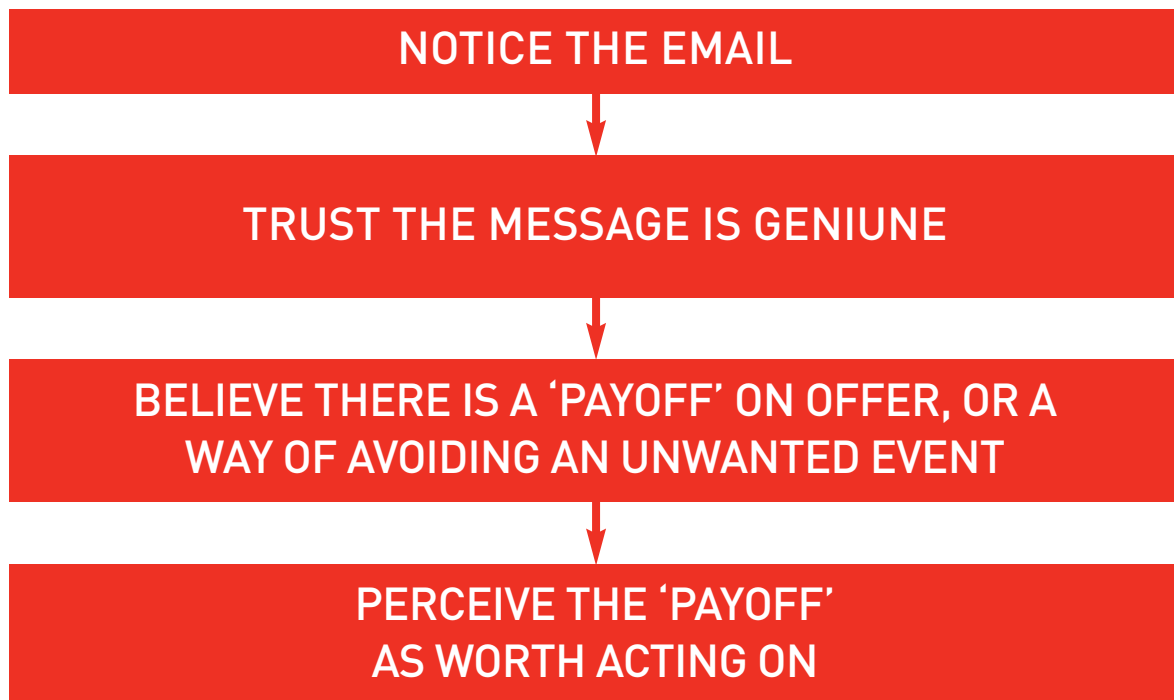
To reduce our scepticism, cybercriminals work hard to convince us that the email is legitimate and use a combination of psychological tricks to do this.

They first focus on drawing us into their 'mind game' and on convincing us that that their "game" is worth playing.

The initial goal of any fraudulent email is to grab our attention by making the email stand out in our crowded inboxes.

Typically, cybercriminals will use headlines to appeal to our personal interests such as 'shopping' or 'dating' and using exclamations or questions in the subject headers.

## The psychological steps of falling for a mind game:



"The target's psychological processing of the information in the message must lead them first to believe that the content is genuine (at which point they will have been deceived); and secondly to believe that there is a reinforcing payoff on offer for responding to the message"

Professor Clive Hollin

**WHEN IS A MESSAGE GENUINE?**

Once they've caught our attention, we must be persuaded that the message comes from a credible, trusted source.

We perceive there is less risk if we believe the source is legitimate, for example if it is from authorities or the law.

It is a well known psychological theory that people are more inclined to trust an authoritative or a familiar/friendly approach.

**THE VOICE OF AUTHORITY**

When we're told to do something by an authoritative figure we tend to do it.

Research has shown that we are highly likely, in the right situation, to be responsive to authority even when the person who purports to be in the position of authority is not physically present.

For example, if an email claims to be from a credit card company and notifies us that our credit card is at risk due to online hackers. Confronting us with the possibility of that our money may be stolen, the email drives us to a fake website to enter our details in return for protection. Clearly the key to the success of this scam is to assure us that it is legitimate.

**ENDORSEMENTS**

Fraudsters also use assurances such as endorsements to manipulate us into trusting that the source is reliable and valid. For example, this may be in the form of product endorsements from other people that have used the website and purchased the product on offer.

Alternatively, scammers put easily recognised and trusted company logos within the text to reinforce the source's legitimacy. Our perception may be strengthened when we know a large company is apparently involved – and so they gain our trust and foster the perception that the message is genuine.

The problem is that most companies legitimately include this sort of reassurance in their interactions with us. This is why scammers can successfully subvert them to trick us out of personal information. In being motivated to do the right thing, we do the exact opposite.

**FAMILIARITY**

We like people who we feel are similar to us. We identify with people who we perceive as having the same characteristics to our own – places of birth, or tastes in sports, music, art, or other personal interests.



It provides a strong incentive for us to adopt a mental shortcut in dealing with that person, to regard him or her more favourably merely because of that similarity. Social networking sites like MySpace, Facebook and Bebo are making it easier for the scammers to mine this personal information for illegal purposes. We freely divulge our nicknames, hobbies, film preferences etc. on these websites giving cybercriminals an instant snapshot to trick us through familiarity.

**FRIENDLY BANTER**

The average PC user wouldn't think twice about trusting an email that came from a friend and swiftly click on a link or open an attachment.

However, some spam software can now pull the names from address lists off messenger accounts. Cybercriminals can use these addresses to target unsuspecting users and get them to divulge information or download malware without a second thought.

Another new technique used by fraudsters is to 'scrape' personal information and contacts from social networking sites and sell them to be used in mass spam attacks.

## MOTIVATING US TO CLICK ON A LINK OR OPEN AN ATTACHMENT

After grabbing our attention and winning our trust, we need to be motivated or encouraged to act and click on a link or open an attachment.

In classic behavioural psychology there are two types of “payoff” that influence our behaviour.

Typical email scams will contain essential elements that play on and exploit these human psychological vulnerabilities “Click here for a reward” or “Click here to avoid something you don’t want to happen”.

### CLICK HERE FOR A REWARD AND GAIN

The first is when we perceive our actions will lead to some sort of gain or reward. The ‘approach’ (as it is known) motivates us and influences our behaviour making us do something.

The rewards on offer may be concerned with personal and intimate relationships, with the availability of contact with, say, other lonely and single people. Alternatively, for those who dare, the offer of sexual experiences for all tastes.

The web is an excellent vehicle for fraud: a few clicks of the mouse and financial reward will follow. Although the medium is electronic, the nature of the fraud may not be new to the Internet. The classic frauds perpetrated through web-based scams include ‘Pump and Dump’, ‘Pyramid Selling’, ‘Risk Free Investment Opportunities’, and ‘Offshore Investments’.

If we think an item is in short supply or available for only a short time, the more we want it. This is one way cybercriminals manipulate us into triggering their desired behaviour.

This type of ‘now or never/don’t lose this opportunity’ offer may apply to investment opportunities, goods, tickets or, indeed, any other commodity. There may be online auctions offering the opportunity to bid for the rare prize.

### CLICK HERE TO AVOID AN UNWANTED EVENT

The second is when we act to avoid an unwanted event – material loss (money), personal loss (poor health or feelings of embarrassment), or social (losing friends or social status). This ‘avoidance’ motivates us to act in a certain way.

Rather than a tangible reward, the scam may play on our fear of loneliness by promising the chance to meet someone through an online dating service (‘why spend another week lonely?’) or fear of unemployment with the chance of work (‘I’m looking for 15 people who are serious about making money working from home’).

Alternatively, the fraudster may play the mind game which offers to alleviate our worries about personal concerns such as body weight, sexual prowess, physical health (‘wish your old energy could come back? Try our new revolutionary health product’) and our appearance. They may also equally play on embarrassment by offering to alleviate our financial worries and debt or to provide us products we’d rather receive remotely than face-to-face!

Some of us are naturally more motivated to achieve positive goals, while others more motivated to avoid negative outcomes. Those of us with glass half full outlook on life will be pre-disposed to acting on a reward payoff, while those of us with a glass half empty outlook will tend to go for an avoidance payoff. All this plays a part in explaining why some of us fall for certain types of online scams and others don’t.

## CURIOSITY GAVE ME A VIRUS

Unfortunately, most of us are born with a healthy degree of curiosity. An email of intrigue, oddity or rarity, can get the better of us – even despite the fact that alarm bells may be ringing.

In fact, a security researcher recently ran an experiment using a reverse social engineering tactic to see just how many people would be curious enough to click through to an online ad that promised to infect your computer upon clicking the link.

Entitled ‘drive-by download’, the site was actually harmless, but more than 400 people did in fact click the link, many presumably driven simply by a desire to see what a virus actually looks like. This shows how common curiosity can be our downfall – and the potential windfall of cyber-scammers.



## MIND GAMES: A CONSTANTLY EVOLVING THREAT ⊗



**Like con men on the street devising new tricks, Internet fraudsters need a never-ending supply of ways to persuade victims to open an attachment, click on a link, or innocently enter personal information on a web page. Bypassing mental barriers, as opposed to software security, is the surest way to pickpocket personal identities and online bank accounts.**

Smart cybercriminals spend valuable time researching the psychological push-buttons of potential targets. They watch news headlines for emotional or worrisome world events or major world sporting events that they can piggy-back on and constantly look for new and novel ways to persuade users to open documents or click links that download threats such as backdoor trojans and spyware onto PCs.

For example instead of directly asking the user to enter personal information into a bogus website, cybercriminals are embedding code into fake news articles and business-orientated "requests for proposals". When opened they install a backdoor onto the PC, then record and transmit the user's keystrokes – including sensitive information.

Recently, a malware author also took to targeting unsuspecting consumers via Google, the world's largest online search engine. It used an assumed-legitimate sponsored advertising link to re-direct users to a malicious site which ultimately downloaded a trojan able to steal online banking credentials. A clever means of acquiring information – the user motivated to act by his interest in the original advert and the assumed safety of Google.

Likewise, scammers are capitalising on new social trends. The MySpace and Facebook generation are failing to question the legitimacy of emails or links.

MySpace was subject to a phishing scam in 2006. The attack started when users were sent a link through an instant messaging program. The link was from someone in their contact lists, asking them to click the link to MySpace to view photos. The link led to a fraudulent MySpace login page. Once the victim entered their information, they were then transparently logged into the real MySpace pages. But in the meantime, all their log-in information became the property of the phisher.

Cyber-scammers are also now thinking beyond purely online mind games. They are manipulating our vulnerabilities through mobile phones.

"SMiShing" (phishing via SMS), is a recent phenomenon that takes the concept and techniques of phishing via email and translates it to text messages.

Scammers send SMS messages to phone users directing them to websites with the reward or avoid payoff. For example, the text will say 'go here to download free security software' or claim that they've been signed up to a dating service at a charge per day and that they need to visit a website to uninstall. Needless to say, the websites they subsequently visit contain malicious content.

This works by diverting our attention because the initial approach comes not through the PC but through the phone – and we still regard our mobile phones as relatively safe.

Cyberscams are often not much more complex than age-old cons run by offline grifters. They are about tapping into the mindsets of their victims and using subtle and sophisticated tricks and triggers to con them.

Increasingly it's the psychological smartness, not code-writing skills that make for a successful cybercriminal.

**"Perpetrators of crime learn from experience and become increasingly sophisticated: they learn what techniques are successful, who falls for what, what bypasses security, and so on."**

Professor Clive Hollin

There are increasing numbers of cyber-thieves out there looking for their next successful scam and the threat is not going away. We therefore all need to be aware that almost everyone can be gullible and vulnerable at least some of the time – and we should realise that we each need to take responsibility and action.

Here are some simple steps we can all take to help defend ourselves from the cyber-scammers.

### TOP TIPS TO HELP AVOID THE ONLINE SCAMS:

#### BE VIGILANT

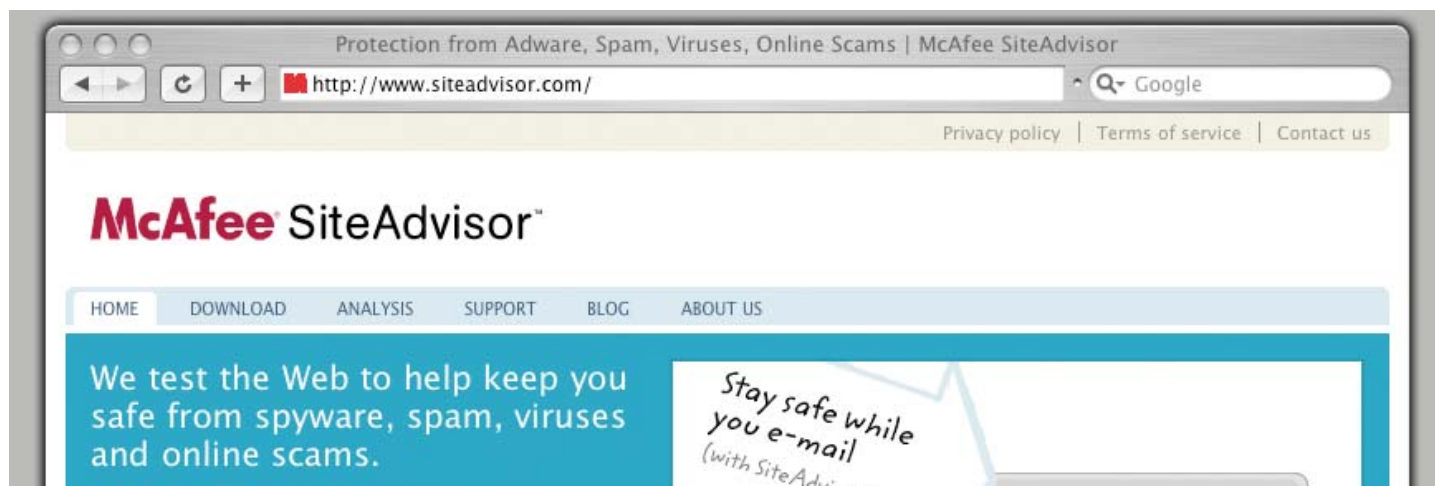
- Be suspicious of any email with urgent requests for personal financial information
- Avoid filling out forms in email messages that ask for personal financial information
- Your bank will never ask for your password or PIN number over email. If you receive such a request, delete the email
- Always err on the side of caution. If you are not sure if an email is legitimate, call the company or bank to confirm the authenticity
- Never click on a link to unsubscribe to an online service before checking that you actually signed up to it first
- In fact, never click on a link in any email even if it looks ok. It is safer to type it in yourself or cut and paste it from the email into your web browser.

#### STAY WEB SAVVY

- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser
- Keep a separate credit card for online purchases so if anything happens you can see it straight away
- Make sure your credit card offers online protection and has a low limit
- Remember not all scam sites will try to show the "https://" and/or the security lock. Get in the habit of looking at the address line, too. Were you directed to PayPal? Does the address line display something different like "http://www.gotyouscammed.com/paypal/login.htm?".

#### KEEP YOUR TECHNOLOGY UP-TO-DATE

- Ensure that your browser is up to date and security patches applied – technology can't protect you from 'Mind Games' but they can identify the security and authenticity of websites
- Invest in a spam filter which will block many types of fraudulent emails
- Download McAfee SiteAdvisor for free which identifies potentially dangerous web sites that have engaged in 'social engineering' attacks, such as spyware, adware, spam, browser attacks, and online scams using intuitive red, yellow, and green icons.





## METHODOLOGY

### ABOUT MCAFEE AVERT LABS

### ABOUT PROFESSOR CLIVE HOLLIN

#### METHODOLOGY

McAfee's Avert Labs team identified real examples of common email scams to be analysed by Professor Hollin for the Mind Games study.

The samples came from the McAfee Spam Traps – a global network of hidden honey pots that the Anti-Spam Research team use to collect huge amounts of spam and phishing samples in real-time.

#### ABOUT MCAFEE AVERT LABS

McAfee Avert Labs is one of the top-ranked security threat and research organisations in the world, employing researchers and engineers in twenty-three cities on five continents and in sixteen countries. The team combines world-class malicious code and anti-virus research with intrusion prevention and vulnerability research expertise.

#### ABOUT PROFESSOR CLIVE HOLLIN

Professor Clive Hollin is Head of the School of Psychology at Leicester University in the UK.

His research interest is in the interface between psychology and criminology. He holds a BSc and PhD in psychology and is a Chartered Forensic Psychologist and Fellow of The British Psychological Society. Clive has been recognised by the Independent on Sunday as being among the ten leading forensic psychologists in Britain.

Clive has authored several books including Psychology and Crime; An Introduction to Criminological Psychology and Criminal Behaviour: A Psychological Analysis.



Professor Clive Hollin