



# Cyber Security: No room for compromise.

**Detective Inspector Paul Peters**  
Regional Cyber Crime Unit  
[RCCU-Tarian@south-wales.pnn.police.uk](mailto:RCCU-Tarian@south-wales.pnn.police.uk)



- Introduction
- Threats
- Protecting Businesses
- How can you assist?
- Questions?



### The Telegraph

Home Video News World Sport **Finance** Comment Culture Travel Life Women Fa  
Companies Comment Personal Finance ISAs Economy Markets Property Enterprise Fi

HOME » FINANCE » NEWS BY SECTOR » INDUSTRY » DEFENCE

## Cyber attacks cost British industry £34bn a year

As well as the multi-billion-pound price tag, the threat from hackers is holding business innovation back, a new report finds

 30   0  444  474  Email



Cyber war: It's a question of when, not if, hackers will attack businesses according to experts Photo: Alamy



By Alan Tovey, Industry Editor

5:00AM BST 10 Jun 2015

 Follow 959 followers



BBC

Sign in



News

Sport

Weather

iPlayer

TV

Radio

## NEWS

Home | UK | World | Business | Politics | Tech | Science | Health | Education | Entertainment

UK | England | N. Ireland | Scotland | Alba | Wales | Cymru

### TalkTalk hack: Llanelli man arrested and bailed

25 November 2015 | UK



An 18-year-old who became the fifth person to be arrested in connection with an alleged data theft from TalkTalk has been released on bail.

- Data breaches are becoming common place and can cost hundreds of millions to rectify with untold reputational damage.
- In 2015 in the UK alone we saw:

<b>Company</b>	<b>Date</b>	<b>No. of Victims</b>
Carphone Warehouse	August 2015	2,400,000
JD Wetherspoon	March 2015	650,000
Scouts Association	January 2015	450,000
TalkTalk	October 2015	156,959

- 2016: Yahoo: 500,000,000 accounts

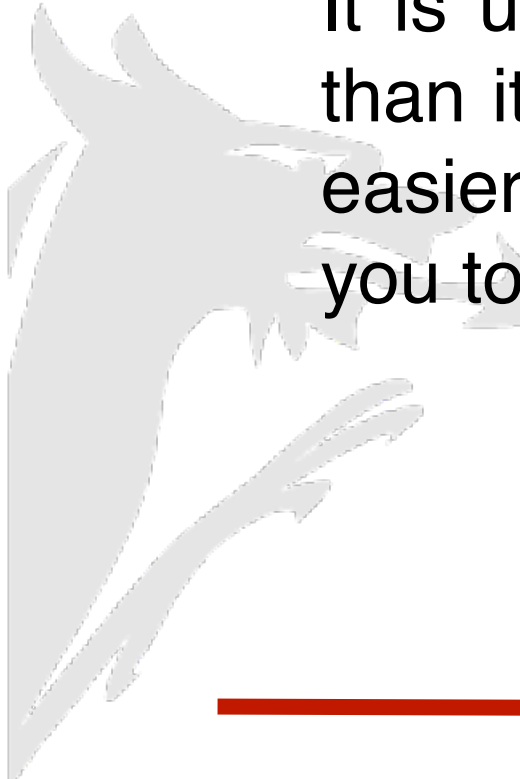
- 2.46 million Cyber incidents & 2.11 million victims of Cyber Crime in a 12 month period between 2014-2015. (Source: ONS)
  - Only 16,349 incidents were reported to Action Fraud during this time period.
  - 60% of small businesses have experienced a cyber breach (Source: KPMG).
  - 94% of procurement managers say that cyber security standards are important when awarding a project to an SME (Source: KPMG).
-

- 
- DDO
  - Wi-Fi



*Social engineering is the art of manipulating people so they give up confidential information.*

It is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. It is much easier to fool someone into giving you their password than for you to try hacking their password!



---







February 12, 2014 · 🌐

HAY HAY GOT MY FLIGHT **TICKETS** NOW...NEW YORK TO  
MANILA...TRAVELLING ON **CATHY PACIFIC**...WILL LAND IN MANILA ON  
18/02/2014 AT 00:05 HRS...HURRAY



40

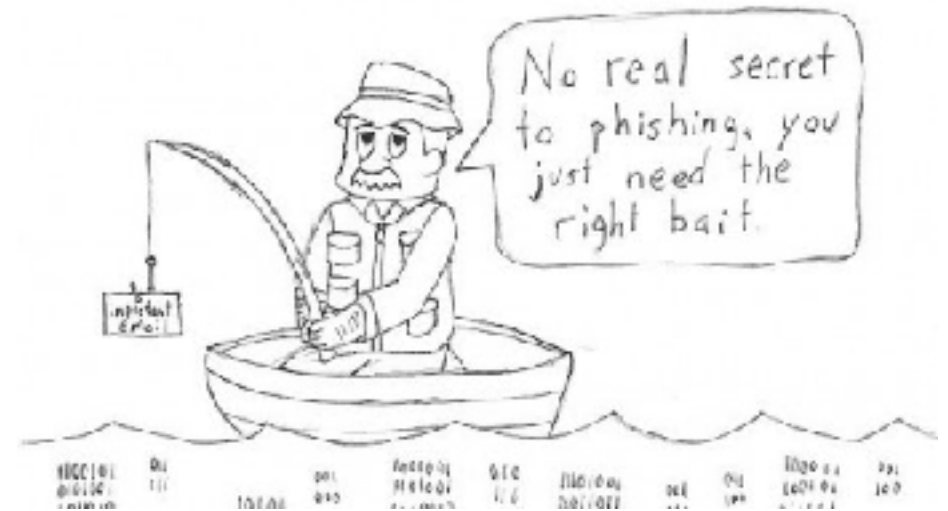
18 Comments 1 Share



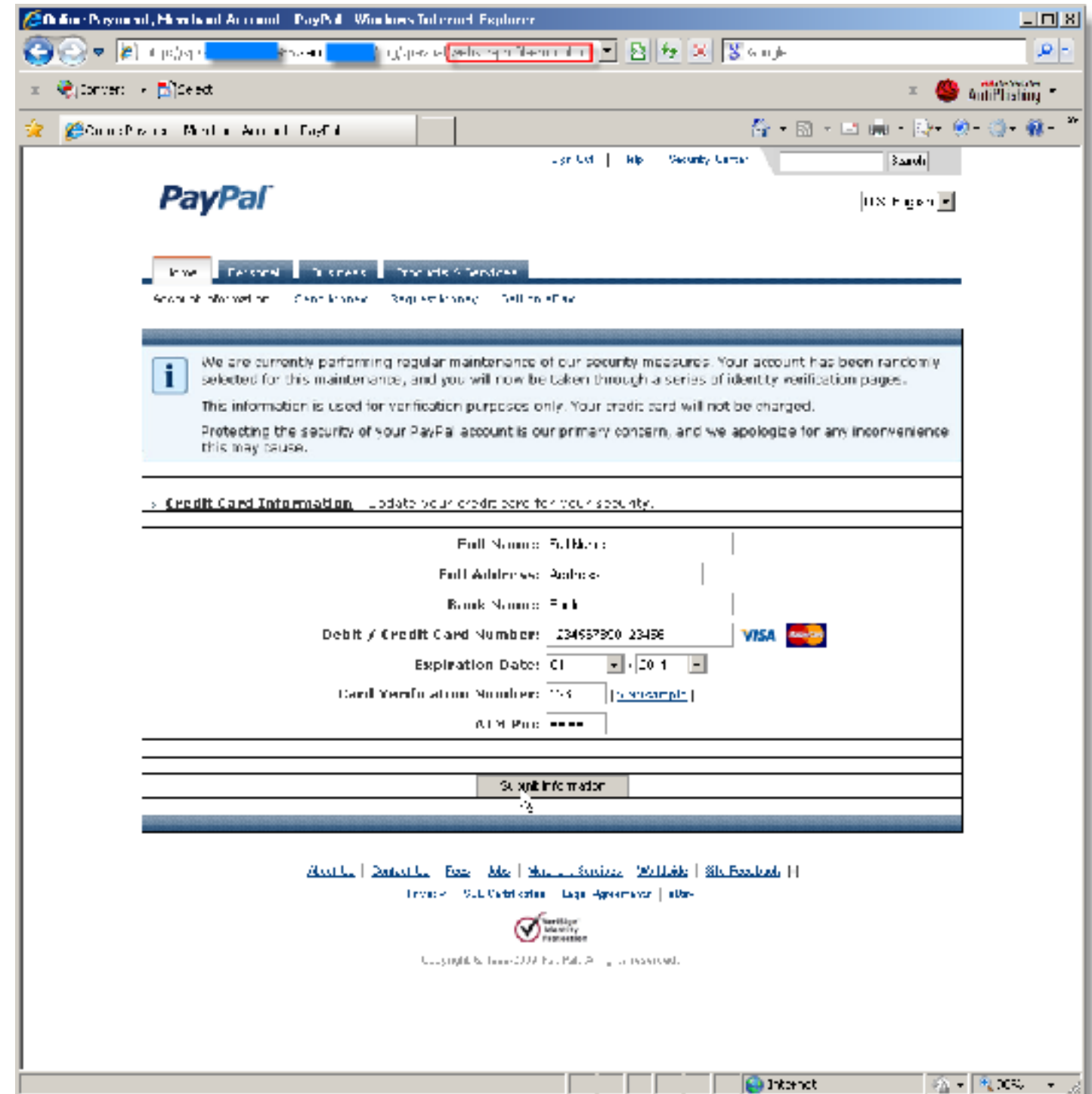
Share



- Disguise the source
- Contains malware / RAT.
- Link to a false website.
- May purport to be from supplier with a request to change contact or bank details.
- Spear Phishing – targeted.



- Victim receives an unsolicited email.
- E.g: PayPal request to follow a link to verify personal details.
- Link directs victim to a rogue website that appears legitimate.
- Bank details and other data is requested.



PayPal - Windows Internet Explorer

PayPal



We are currently performing regular maintenance of our security measures. Your account has been randomly selected for this maintenance, and you will now be taken through a series of identity verification pages. This information is used for verification purposes only. Your credit card will not be charged. Protecting the security of your PayPal account is our primary concern, and we apologize for any inconvenience this may cause.

**Credit Card Information** - Update your credit card for your security.

Full Name: Full Name

Full Address: Address

Bank Name: Bank

Debit / Credit Card Number: 234567890 23456  

Expiration Date: 01/2011 - 12/2011

Card Verification Number: 1234 [\[Example\]](#)


PIN: \*\*\*\*

**Submit Information**

[About Us](#) | [Contact Us](#) | [Privacy Policy](#) | [Terms of Service](#) | [Help](#) | [Feedback](#) | [Sign Out](#)

© 2007 PayPal Inc. All rights reserved.





[Latest](#)  
**Q2 Global Fraud Jumps 50% From 2015**

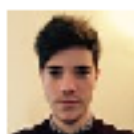
[Home](#)
[News](#)
[Topics](#)
[Features](#)
[Webinars](#)
[White Papers](#)
[Events & Conferences](#)
[Directory](#)

INFOSECURITY MAGAZINE HOME • NEWS FEATURES • ALMOST A THIRD OF STAFF STILL FALL FOR PHISHING EMAILS



17 AUG 2016 NEWS FEATURE

## Almost a Third of Staff Still Fall for Phishing Emails



**Michael Hill** Deputy Editor, Infosecurity Magazine

Email Michael Follow @MichaelInfosec



Almost one third of employees are putting their organization at risk of phishing attacks, according to new research from **Duo Security**.



The firm has released findings from its free phishing simulation tool Duo Insight, which offers organizations of all sizes a free internal phishing drill system that allows them to simulate a phishing campaign on their employees, and found that 31% of staff clicked the link in the emails sent by their internal team. This shows phishing is still a significant threat to companies as they attempt to stem the tide of cyber attacks that continue to plague organizations across the globe.



**Watch now**


Strategy - Insight - Technology



The UK was among the  
top 5 countries affected  
by ransomware in 2015

Symantec - Evolution of ransomware 2015



The estimated number of  
devices infected in one week by  
a single piece of ransomware

<http://www.forbes.com/>

**£514**

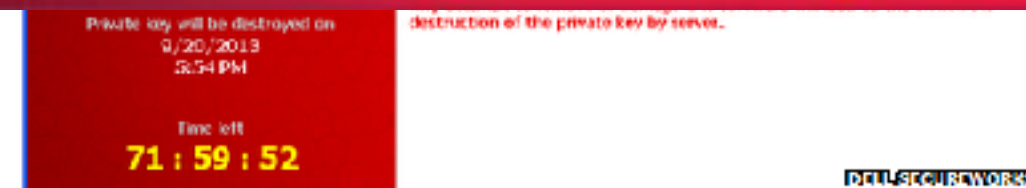
The average ransomware  
demand

Symantec - Ransomware & Businesses 2016





- Failure to pay the ransom and all data is permanently lost



Infected victims are given a time limit to release their data before they lose it forever

A virulent form of ransomware has now infected about quarter of a million Windows computers, according to a report by security researchers.

Related Stories

**NO MORE RANSOM!**[Crypto Sheriff](#)[Ransomware Q&A](#)[Prevention Advice](#)[Decryption Tools](#)[Report a Crime](#)[About the Project](#)

**NEED HELP** unlocking your digital life  
without paying your attackers\*?

**YES****NO**

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

**GOOD NEWS**

Prevention is possible. Following simple cyber security advice can help you to avoid becoming a victim of ransomware.

**BAD NEWS**

Unfortunately, in many cases, once the ransomware has been released into your device there is little you can do unless you have a backup or security software in place.

**GOOD NEWS**

Nevertheless, it is sometimes possible to help infected users to regain access to their encrypted files or locked systems, without having to pay. We have created a repository of keys and applications that can decrypt data locked by different types of ransomware.

At the moment, not every type of ransomware has a solution. Keep checking this website as new keys and applications are added when available.



## Attacker



## Bots

### Server Application Unavailable

The web application you are attempting to access on this web server is currently unavailable. Please hit the 'Refresh' button in your web browser to retry your request.

**Administrator Note:** An error message detailing the cause of this specific request failure can be found in the application event log of the web server. Please review this log entry to discover what caused this error to occur.

## Victim

## **DDoS attacks on sale for \$2 an hour**

Burgeoning marketplace for cybercrime tools and services means cybercriminals need no longer be tech savvy, study finds

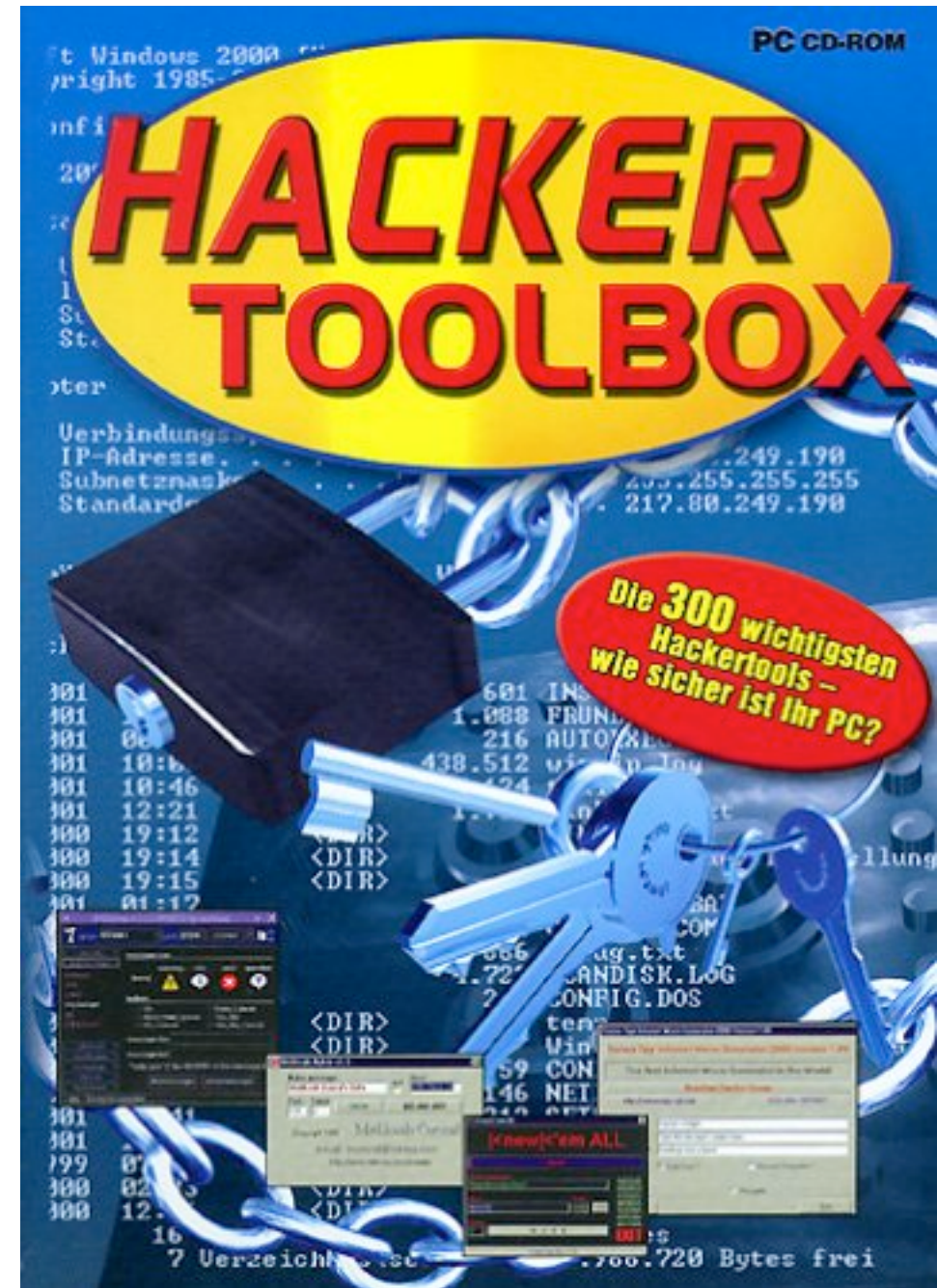


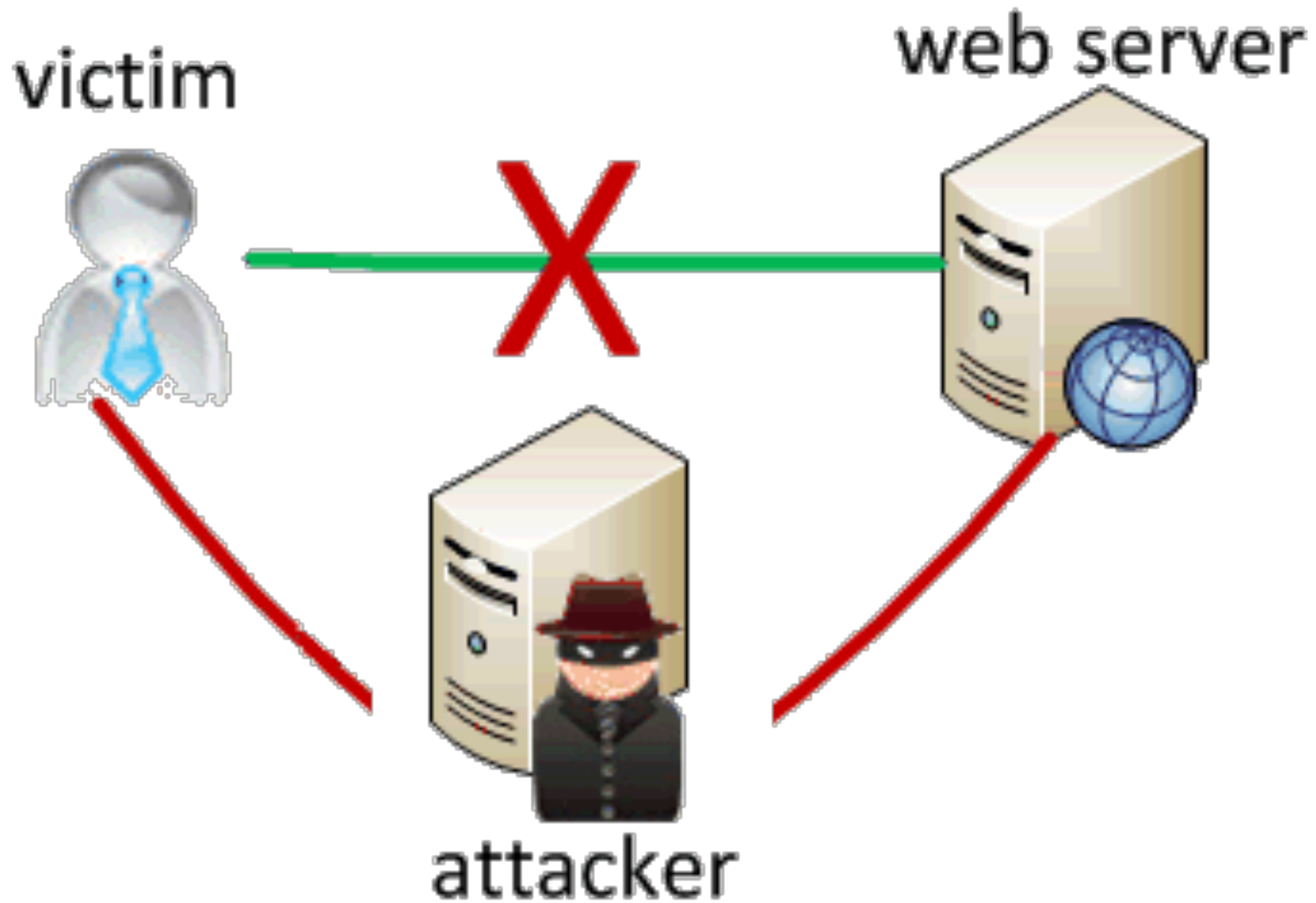
Cybercriminals can now purchase DDoS attacks for \$2 (£1.32) an hour from a rampant online marketplace of tools and services.

That is according to a new white paper analysing the growth of the "as-a-service" nature of cybercrime penned by two senior technical bods at security vendor McAfee.

The study seeks to shatter the perception that all cybercriminals are technical masterminds. Instead, all they need to bring a global corporation of their choosing to its knees is a credit card.



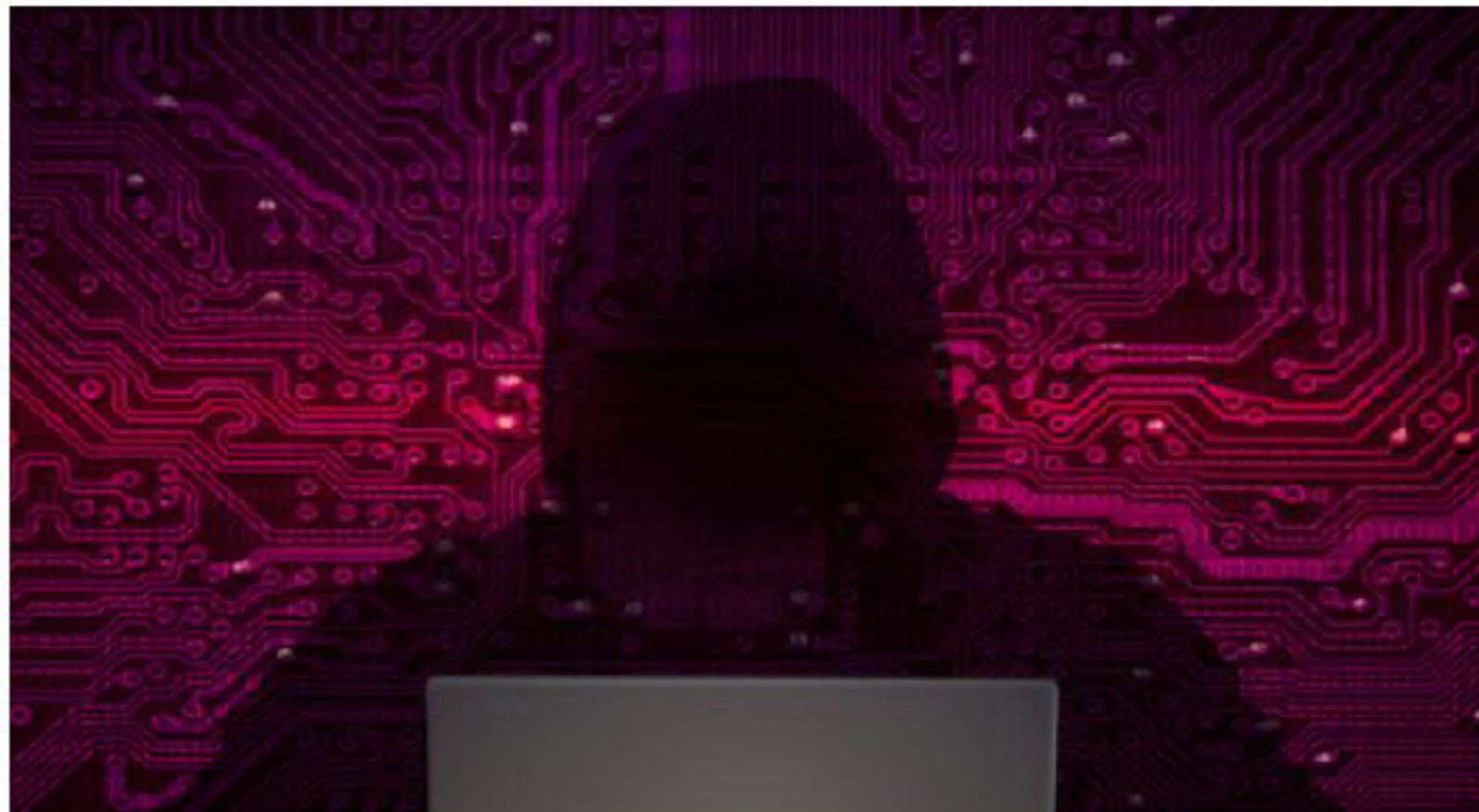






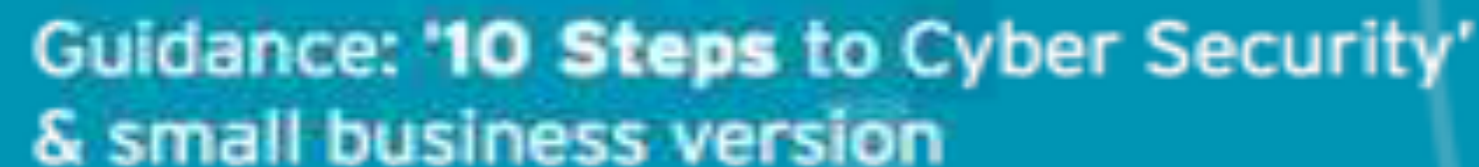
## **SMBs vulnerable to cyber-crime due to lack of resources, warns report**

Webroot report suggests that only 37 per cent of SMBs feel 'completely ready' to combat cyber-threats



Most small and medium-sized businesses (SMBs) are vulnerable to cyber-attacks and hackers because they don't have sufficient resources to protect themselves.







## Cyber-security Information Sharing Partnership

- National CiSP launched March 2013.
- All Wales Regional CiSP launched November 2015, championed by Airbus
- Joint industry & Government scheme administered by CERT-UK.
- CiSP is an online social networking tool to exchange information on threats and vulnerabilities.

- Engagement with industry and government counterparts in a secure environment
- Early warning of cyber threats
- Ability to learn from experiences, mistakes and successes of others and seek advice
- Access to content - including vulnerabilities and latest incidents.
- CiSP is **free** to join for any organisation that has responsibility for a UK-based IT network.





[Inbox](#) [Feeds](#) [History](#) [Bookmarks](#) [Settings](#) [Logout](#)

[Home](#) [Content](#) [Members](#) [Places](#) [Create](#)

### Advisory - Quadrooter vulnerability affecting Android

Advisory articulating a number of vulnerabilities discovered affecting Android phones using Qualcomm chipsets - thought to be in the region of one billion devices



○○○●○



[Sign up](#) for the CERT-UK Network Reporting (CNR) services tailored to your organisation.



Update your [profile](#) and set your [preferences](#) to receive email notifications to ensure you see the information you want.



[Report an incident](#) to CERT-UK or visit our [Support Pages](#) for user guidance.

## What's Happening

[view feeds](#) ^

[All](#) [Popular](#) [Following](#)



New Post "Office macro malware - in Microsoft Publisher files"  
by [KevinB2@princeslimited](#)

Green

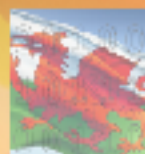


Comments posted on "Linux security updates"  
by [john@defensevizard](#) in Vulnerabilities

White

## Welcome to CiSP





## Wales Group

[Follow](#)
[Overview](#) [Activity](#) [Content](#) [People](#) [Reports](#)

### GROUP OVERVIEW



On behalf of CERT-UK, TARIAN, ROCCU and Group Champions Arthia, we welcome you to your private group on CiSP. This has been established to provide companies in Wales with a private area on CiSP to share information about cyber threats and vulnerabilities. Any information you share in this group will only be visible to other members of the group, and the CiSP Fusion Cell. However, we would encourage you to share relevant information more widely in order to benefit all CiSP members. The success of the group will depend on the level of participation of its members and we would therefore encourage you to share information regularly, posing questions and providing feedback, using the 'like' button and 'rating' feature is also encouraged. We welcome feedback on how the group is working and what

### RECENT ACTIVITY



Shared by PaulP1@Tarian  
2 hours ago [Show more](#)



### New Ransomware - FANTOM

New ransomware is being reported that works by displaying a fake Windows Update screen that creates the impression that a new critical update is being installed. In the background the users files



EddieM@Tarian in Wales Group  
2 hours ago [Show more](#)



### Cybercrime-as-a-Service Explodes Onto the Scene



Interesting article, Cybercrime as a Service Poses a Growing Challenge September 4, 2016 | By Rick M Robinson (<https://securityintelligence.com/authors/rick-m-robinson/>) A few years ago

Liked (1) · [Comment](#) · [Share](#)



Craig G0@Tarian in Wales Group  
3 hours ago [Show more](#)

## National Initiatives:





The Cyber Essentials Badge allows your company to advertise the fact that it adheres to a government endorsed standard.

There are two levels of badges that your organisation can apply for:



### **Cyber Essentials**

Requires the organisation to complete a self-assessment questionnaire, with responses independently reviewed by an external certifying body.



### **Cyber Essentials PLUS**

Tests of the systems are carried out by an external certifying body, using a range of tools and techniques.

Whether your organisation seeks to attain either of these or simply to self-assess and apply the controls will depend on your business drivers and the level of rigour you need or want to demonstrate.

Cyber Essentials documents are FREE to download and any organisation can use the guidance to implement essential security controls, but some may want or need to gain independent assurance that they have fully deployed the controls. Organisations that have been successfully independently assessed or tested through the scheme's assurance framework will attain a Cyber Essentials certification badge. This will help you demonstrate to customers, partners or clients that your company takes cyber security seriously - boosting reputations and providing a competitive selling point.



Cyber Essentials concentrates on five key controls:

1. **Boundary firewalls and internet gateways** - these are devices designed to prevent unauthorised access to or from private networks, but good setup of these devices either in hardware or software form is important for them to be fully effective.
  2. **Secure configuration** - ensuring that systems are configured in the most secure way for the needs of the organisation.
  3. **Access control** - Ensuring only those who should have access to systems to have access and at the appropriate level.
  4. **Malware protection** - ensuring that virus and malware protection is installed and is up to date.
  5. **Patch management** - ensuring the latest supported version of applications is used and all the necessary patches supplied by the vendor been applied.
-



Get Safe Online  
Free expert advice

[Home](#) | [About Us](#) | [Partners and Supporters](#) | [Press](#) | [News](#) | [Blog](#) | [Jargon Buster](#) | [Contact](#)

Follow us



Google™ Custom Search



Personal

Business

Hardware  
and Devices

Information  
Security

Online Safety  
& Security

Rules, Guidelines  
& Procedures

Software

Ways  
You Work

Personal

# Cyber Security

## Underpinning the digital economy

Attack

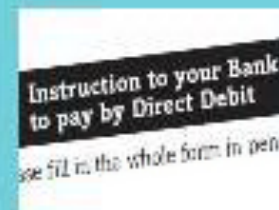
*Businesses need to "get real" about cyber security*

[Read more...](#)



*New cyberattack  
extortion threat to  
businesses*

[Read more...](#)



*Increase reported in  
mandate fraud*

[Read more...](#)



*Alarming increase in CEO  
impersonation fraud*

[Read more...](#)



*SMEs warned about  
increase in invoice fraud*

[Read more...](#)



BE **CYBERSTREETWISE**

[Secure your online devices >](#)

[Protect your online privacy >](#)

[Look after your money online >](#)

[Defend your business >](#)

[Home](#) > [Important IT Policies for your Business](#)


Share this page:




# Important IT Policies for your Business

On this page:

- [Password policies](#)
- [User privileges](#)
- [The Data Protection Act](#)
- [Protecting sensitive data](#)
- [Personal devices](#)

 Most businesses now use some sort of computer device which is most likely linked to a network. Having appropriate IT policies and procedures for your business will make it less vulnerable to attacks and more likely to comply with the Data Protection Act.

 Find out more about managing access to your IT systems as well as protecting your network when workers use their own devices.



# 10 Steps To Cyber Security



Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

## Network Security



Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

## Malware Protection



Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

## Monitoring



Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

**Maintain the Board's engagement with the cyber risk.**

## Incident Management



Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

**Establish an effective governance structure and determine your risk appetite.**

**Information Risk Management Regime**



## User Education and Awareness

Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.



## Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

## Secure Configuration



Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

## Removable Media Controls



Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to the corporate system.

## Managing User Privileges



Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.



- **ActionFraud**

- National Fraud & Cyber Crime Reporting Centre

-  **0300 123 2040** 

[www.actionfraud.police.uk](http://www.actionfraud.police.uk)

---



