PROFiT

Prevention of Fraud in Travel

THE COUNTER FRAUD CAMPAIGN 2019

INDEX

PROFiT is the only official travel industry counter fraud body. We work on your behalf to carry out analysis and research, disseminate best practice and disrupt crime.

Find out how you can join the fight against crime. Contact via: contactus@profit.uk.com

PROFiT

GLOSSARY OF TERMS

ACAS	The Advisory, Conciliation and Arbitration Service	A Crown non-departmental public body of the Government of the UK. Its purpose is to improve organisations and working life through the promotion and facilitation of strong industrial relations practice.
ACFE	The Association of Certified Fraud Examiners	A US organisation of fraud examiners.
ACTION FRAUD		The UK's national reporting service for fraud and financially motivated cybercrime.
COLP	City of London Police	The territorial police force for the City of London (the square mile). The smallest force in the UK.
CPNI	Centre for the Protection of the National Infrastructure	The United Kingdom government authority which provides protective security advice to businesses and organisations across the national infrastructure.
CSP	Content Security Policy	A computer security standard introduced to prevent cross-site scripting, clickjacking and other code injection attacks resulting from execution of malicious content in the trusted web page context.
DDoS	Distributed Denial of Service Attack	Cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.
DKIM	DomainKeys Identified Mail	An email security policy that stops the contents being altered during transit.
DMCA	Digital Millennium Copyright Act Services	A service that criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works.
DV	Domain Validation	An X.509 digital certificate typically used for Transport Layer Security where the domain name of the applicant has been validated by proving some control over a DNS domain.
EV	Extended Validation Certificate	An SSL certificate conforming to X.509 that proves the legal entity of the owner and is signed by a Certificate Authority key that can issue EV certificates.
FBI	Federal Bureau of Investigation	The domestic intelligence and security service of the United States and its principal federal law enforcement agency.
FCA	Financial Conduct Authority	The conduct regulator for 59,000 financial services firms and financial markets in the UK and the prudential regulator for over 18,000 of those firms.
GCA	Global Cyber Alliance	An international, cross-sector body dedicated to eradicating **cyber** risk and improving the connected world.
FIN	Fraud Intelligence Network Ltd	A private company that operates the FIN Intelligence System
HMIC	Her Majesty's Inspectorate of Constabulary	The independent inspection body that assesses police forces and policing, asking the questions that citizens would ask and publishing information to allow the public to compare the performance of their force against others.

© Prevention of Fraud in Travel 2019

HTML		Hyper Text Markup Language		The standard mark-up language for documents designed to be displayed in a web browser.
HTTPS		Hypertext Transfer Protocol Secure		A protocol used to provide security over the Internet. A website conforming to the HTTPS protocol shows a green padlock in the site identity button to the left of the address bar and has the letter 'S' after the abbreviation HTTP both of which designate that it is secure.
ICANN		The Internet Corporation for Assigned Names and Numbers		A non-profit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation.
ISP		Internet Service Provider		An organization that provides services for accessing, using, or participating in the Internet.
JavaScript				A high-level, just-in-time compiled, object-oriented programming language that conforms to the ECMAScript specification.
JMLSG		Joint Money Laundering Steering Group		A body formed from financial services trade bodies in the UK which promotes best practice to counter money laundering.
KYC		Know Your Customers		The process of a business verifying the identity of its clients and assessing their suitability, along with the potential risks of illegal intentions towards the business relationship.
MFA		Multi-Factor Authentication		More than one level of authentication to gain access to
MITM		Man-In-The-Middle Attack		Data theft occurring when you send data across the internet and an unauthorised third person in between you and the recipient intercepts it.
NCA		National Crime Agency		The UK agency against organised crime; human, weapon and drug trafficking; cybercrime; and economic crime that goes across regional and international borders
NFIB		National Fraud Intelligence Bureau		Operated by the COLP the NFIB helps the police and their partners catch and disrupt criminals and make the UK a more fraud-resistant society, by alerting our communities to threats from fraud and working together to prevent crime occurring.
OV		Organisation Validation		The standard type of certificate required on a commercial or public facing website. OV certificates conform to the X.509 standards and thus contain all the necessary information to validate the organization.
OCG		Organised Crime Group		A category of transnational, national, or local groupings of highly centralised enterprises run by criminals to engage in illegal activity, most commonly for profit. Some criminal organisations, such as terrorist groups, are politically motivated.
PROFiT		Prevention of Fraud In Travel Ltd		A not-for-profit company that specialises in disrupting crime, carrying out research and analysis as well as designing crime out of all business types.
PHP		Hypertext Pre-Processor		
SSIDs		Service set Identifier		The name assigned to a wireless network using case sensitive characters strings up to 32 characters in length.
SHODAN		Sentient Hyper-Optimised Data Access Network		A search engine type which can identify unsecured devices.
SMTP		Simple Mail Transfer Policy		The protocol that allows emails to be sent and received across the internet
SPF		Sender Policy Framework		E-mail return path value validation policy
SQL		Structured Query Language		A domain-specific language used in programming and designed for managing data held in a relational database management system, or for stream processing in a relational data stream management system.
SSL		Secure Sockets Layer		A cryptographic protocol designed to provide communications security over a computer network.
TLS		Transport Layer Security		TLS has now largely replaced SSL as a cryptographic protocol designed to provide communications security over a computer network.
VPN		Virtual Private Network		An extension of your own private network across the public network enabling users to send and receive data across shared public networks as if they were diredctly connected to their private network.
XSS		Cross Site Scripting		A general-purpose programming language originally designed for web development.

PROFIT

RECOMMENDED PLACES TO OBTAIN SUPPORT & INFORMATION	
CPNI A source of free expert guidance on cyber security matters	https://www.cpni.gov.uk
Digital Millennium Copyright Act Takedown A service that badges, protects and takes down copies of your website	https://www.dmca.com/faq/What-is-a-DMCA-Takedown
GCA Small Business Toolkit Use the GCA Cybersecurity Toolkit to assess your security posture, implement free tools, find practical tips, and use free resources and guides to improve your company's cybersecurity readiness and response.	https://gcatoolkit.org/smallbusiness/
National Cyber Security Centre Official advice and solutions from GCHQ on many aspects of cyber security and vulnerabilities	https://www.ncsc.gov.uk/section/advice-guidance/all-topics
Netsparker (Free community edition and trial version available). Good for testing SQL injection and XSS.	https://www.netsparker.com/web-vulnerability-scanner/
OpenVAS Claims to be the most advanced open source security scanner. Good for testing known vulnerabilities. But it can be difficult to setup and requires an OpenVAS server to be installed which only runs on *nix	http://www.openvas.org
SecurityHeaders.io (free online check). A tool to quickly report which security headers mentioned above (such as CSP and HSTS) a domain has enabled and correctly configured	https://securityheaders.com
Symantec Endpoint Protection Norton Internet Security and Symantec Endpoint Protection are both security software suites made by the same company, Symantec, but aimed at different audiences. Many of the security features are very similar or identical across the two suites. The website has a number of free resources available.	https://www.symantec.com/en/uk/security-center/threats
Xenotix XSS Exploit Framework A tool from OWASP (Open Web Application Security Project) that includes a huge selection of XSS attack examples, which you can run to quickly confirm whether your site's inputs are vulnerable in Chrome, Firefox and IE	https://xenotix.in

PROFIT

INDEX

Subject	Edition	Page
A		
Accounting Fraud	3	3
ACAS	5	3
ACFE	3	1
Action Fraud	7	1
Address Resolution Spoofing	18	4
Adoption Certificate	4	2
Adware	17	2
	20	2
Application Registration Card	4	2
Anti-Malware Software	20	2
Anti-Spyware Software	20	2
Anti-Virus Software	20	2
Asset Misappropriation	3	2
B		
Backdoor	17	3
Backups		
- Differential, Full, Incremental and Mirror	20	3
Bandwidth	15	2
Bank Statements	4	2
Birth Certificate	4	2
Bogus Invoices	12	2
Bogus Payment Requests	12	3
Booking – Review The Details	9	2
- Confirming The Details	9	3
Booters	15	2
Bots	10	1
	17	3
Brand Appropriation	12	1
- Social Media	12	2
- Websites	12	1
Bribery Act 2010	3	1
Brute Force	19	3
Business Address	4	2
Business Name	4	2
Business Rate return	4	2
C		
Call For Service	4	2
Cardholder Not Present Fraud	7	1
Cash Flow (Origin Or Destination)	9	1
Caution	4	2
CERTs	7	1
Certificate of Incorporation	14	4
Chargeback	15	3
- Challenging	2	2
Checks On All New Recruits	11	1
Child Protection Considerations	11	3
Citrix	2	1
City of London Police	18	2
Civil Cases	1	4
Civil Judgements	8	3
Cloned – Protect Your Website From	2	1
Company Checks	4	3
Company Directors Disqualification Act 1986	14	3
Company Registration	3	2
	4	1
Computer Misuse Act 1990	3	2
Consumer Credit Act 1974, Section 75	15	1
Consumer Protection Act 1999	11	1
Copyright Notice	14	4
Copyright Website Pages	13	3
Copyscape	14	3
Corruption	14	3
Court – Attendance	2	1
- Dressing For	8	3
- Procedure	8	3
Court Of Session	8	3
Credit History	8	4
Crime Reviewers	2	3
Criminal Cases	7	3
Criminal Convictions	8	3
Cross Site Scripting	2	3
Crown Court	15	4
Cryptolocker	8	4
CSIRTs	17	3
	14	4
Cybersquatting	15	3
	14	3
D		
Data Breaches	19	4
DDoS Attack	15	1
Defence	8	3

Subject	Edition	Page
Digital Fingerprint	13	4
Disabling The Right Click	13	2
Disciplinary Process	5	2
Divorce Papers	4	2
DMCA Content	13	1
DMARC	4	3
DNS Spoofing	17	2
Driving License (UK)	18	4
Dunn & Bradstreet Reports	4	2
	4	2
E		
E-mail Security	20	3
- DKIM	20	4
- DMARC	20	4
- SMTP	20	4
- SPF	20	4
Employees – Arrest	6	3
- Interview	6	3
Encryption	13	4
Entitlement Letter	4	2
Equivalent Foreign Body	4	2
Escalation And Response Policy	14	4
Evidential Reports	8	2
F		
Fair Billing Act 1974	11	1
Fingerprinting	13	4
Firearms Certificate	4	2
Firewall	16	4
	20	1
Flashdrives	18	1
Foreign Powers	15	3
Form 12	4	2
Form Of Authorisation	14	3
Friendly Fraud	11	2
Fraud – Detection	6	1
- Investigate	6	1
- Some Signs Of Fraud	6	1
When A Fraud Is Happening	7	2
G		
General Misconduct	5	2
Google Alerts	13	2
	14	3
Gross Misconduct	5	1
		2
		3

Subject	Edition	Page
H		
Hackers	15	3
	15	6
Hacktivists	16	1
Hashing	19	5
HM Forces ID Card	4	2
Holding Company	4	2
Home Office	7	3
Home Affairs Select Committee	7	3
HTTP	18	4
HTTPS	15	5
	18	5
	20	4
Human Resources (HR)	5	1
	5	2
I		
ICANN	14	1
Identification	4	1
Identifying Fraud Risks	1	1
Identity	2	2
Identity Of Directors, Partners, Shareholders, Company Representatives	4	2
Industry Requirements	7	4
Interception	19	3
Internal Fund Diversion	12	3
Implicated Employees	6	2
Incorporation Date	4	2
Inland Revenue Tax Notification	4	2
Industry Membership	4	2
Internal Business Documents	4	2
Invoices/Receipts/Bills	4	2
ISP	15	3
J		
Joint Money Laundering Steering Group	4	3
K		
Kensington Port Lock	18	2
Keylogging	17	3
	19	3
Know Your Supplier	18	2
	4	3
L		
Legitimate Purpose	4	2
Local Suspect	7	2

© Prevention of Fraud in Travel 2019

Subject	Edition	Page
Log Of Records	4	3
Logic Bomb	17	3
Lone Operators	1	1
M		
Mackenzie Friend	5	2
Magistrates Court	8	3
Malicious Actors	14	4
Malvertising	17	3
Malware	17	2
Man-In-The-Middle Attack	18	3
Manual Guessing	19	3
Marriage Certificate	4	2
Mastercard SAFE	10	2
mDNS Spoofing	18	4
Memory Stick	18	1
Multi Factor Authentication	19	4
Multi Step Authentication	14	2
N		
National Crime Agency	1	1
O		
Obligation To Report A Fraud	6	3
Organised Crime Groups	1	1
P		
“Packages”	7	3
Packet Sniffer	18	3
Parent Company Or Entity	4	2
Partnership Deeds	4	2
Passport (signed)	4	2
Passwords		
- Blacklisting	19	5
- Change Default	19	5
- Don’t Enforce Regular Expiry	19	5
- Factors That Weaken	19	2
- How They Can Be Compromised	19	3
- Management Software	19	5
- Manage Shared Access	19	5
- Official Advice	19	4
- Single Sign-In System	19	4
- Spraying	19	4
- Strong and Unique	14	2
- System	20	3
- The Basics	19	4
- Three Little Words	19	2
PAYE Records	4	2
Payment Cards		
– How They Work	9	1
- Problems With	9	2
Payment Diversion	12	2
Pen Drive	18	1
Personal Lifestyle	1	1
Phishing	17	1
Politically Exposed Persons	2	4
Pre-Employment Screening	2	1
Preparing For Court	8	1
Preserving Documents	6	2
Proceeds of Crime Act 2002	3	1
Professional Qualifications	2	4
Proof Of Identity	9	3
Prosecution	8	3
Protect Password At Rest	13	1
Protect Password In Transit	19	5
Protect The Access Management System	19	4
Protecting Web Content	19	5
Protecting Web Sites	14	1
Q		
Quad9	17	2
Qualifications	20	4
	2	4
R		
Ransomware	17	3
Records	4	3
Record Keeping	5	4
References	2	2
Report A Fraud	7	1
Residency Permit	4	2
Residential Address	2	2
Right To Work In The UK	2	2
Rogue Address Points	18	4
Rogue Security Software	17	3
Rootkits	17	3
S		
Searching	19	3
Securing Images	13	2
Securing Text	13	2
Security Monitoring	19	5

Subject	Edition	Page
Shadow Brokers	17	1
Sheriff	8	3
Shodan	18	4
Shoulder Surfing	19	3
Social Engineering	19	3
Social Media Organisations	16	4
Spam	17	1
Spearphishing	17	1
	19	4
Spoofing Supplier Details	12	5
Spyware	17	3
SQL Injection	15	4
SSLStrip	18	4
Stealing Passwords	19	3
Stressers	15	2
Sub-Contractors Certificate	4	2
Subsidiary Company Or Entity	4	2
System Monitors	20	3
System Redundancy	15	2
T		
Tax Reference	4	2
Tax Returns	4	2
Taxonomy of Crime Against Travel Organisations	1	2
Terrorist Groups	16	3
Theft of Password Hash File	19	4
Throttling Or Account Lockout	19	4
Tracking Cookies	20	3
Trademark	14	4
Transfer Dispute Policy	14	2
Transfer Lock	14	2
Trojans	17	3
	20	3
Typosquatting	14	4
U		
Unauthorised Data Downloading	18	1
Unauthorised Transfer Complaint	14	2
UK Companies House	4	2
USB Port Locks	18	2
USB Stick	18	1
US Copyright Office	14	3
Utility Bills	4	2

Subject	Edition	Page
V		
Validate A Booking	9	1
Validation Tools	10	2
VAT Number	4	2
VAT Registration/Returns	4	2
Virtual Private Network	18	2
Viruses	17	3
VISA TC40	10	2
W		
Wannacry	17	1
Warrant Card	4	2
Watermark	13	3
Which	7	4
Who Is	14	1
Who Is Data Reminder Policy	14	2
Wi-Fi Pineapple	18	3
Witness Statement	8	1
Work History	2	2
Worms	17	3
X		
Y		
Z		

© Prevention of Fraud in Travel 2019