

Police Hacking notes

Bedfordshire Police force

1 – Hacking

Cleveland Police Force

Hacked

2016/17 – 230

2017/18 – 221

Hacking

2016/17 – 135

2017/18 – 135

Derbyshire

2017

IP believes offender hacked dating site and obtaining details

IP thinks someone has accessed Facebook site and stolen photographs which were later distributed

Offender has hacked into siblings email and facebook account

Expartner has hacked into mobile account and sent indecent photos

Offender has hacked into IP's mobile and bank account and taken small amount of cash

2018

IP's believe that offenders have hacked in to phone and accessed bank details

IP states that offender has hacked email account and set up a facebook profile in their name

IP states that offenders are setting up fake profiles which is affecting their business

IP states the offender has hacked facebook account and removed photographs

IP states that offender has hacked gmail and snapchat account and gained personal information

Dorset

Year	Occurrence Summary	Outcome
2016/17	Cyber Crime - Business Email Has Been Hacked	Victim declines/unable to support action to identify offender
2016/17	Theft Of Client Information By	Police - named suspect, victim supports but evidential difficulties

	Former Employee	
2017/18	Suspicious Circumstances - Website hacked.	Police - named suspect, victim supports but evidential difficulties
2017/18	Possible Hacking Offences	Investigation complete no suspect identified

Nottinghamshire

Incident Closure Type	Financial Year	
	2016/17	2017/18
ABANDONED CALL TO EMERG SERV	2	0
ASB NUISANCE	1	1
ASB PERSONAL	4	4
ASSIST OTHER AGENCY	1	0
BURGLARY OTHER THAN DWELLING	1	0
CIVIL DISPUTE	1	2
CRIME - OTHER	10	10
CRIMINAL DAMAGE	1	0
DOMESTIC INCIDENT	28	47
FRAUD AND FORGERY	33	40
HARASSMENT/STALKING	11	11
HATE INCIDENT	1	0
HOAX CALLS TO EMERG SERVICE	7	16
MENTAL HEALTH	11	29
MESSAGES	19	22
PASSED OTHER AGENCY/FORCE	31	17
SEXUAL OFFENCES	4	7
SUSP CIRC/VEH/INSECURE PREM	34	35

THEFT - OTHER	1	3
VIOLENCE AGAINST PERSON	3	2
Grand Total	204	246

Hertfordshire

Offence by Outcome	2015	2016	2017
Computer - Unauth Access Facilitate Offence			
Charged/Summoned	1		
Investigation Complete No Suspect	2		
Named Suspect Evidential Difficulties	1		
Named Suspect Victim Unsupportive	1		
Computer - Unauth Access to Material with Intent			
Caution - Adults	1		
Charged/Summoned	1		
Investigation Complete No Suspect		2	
Named Suspect Evidential Difficulties		1	
Named Suspect Victim Unsupportive		1	
Computer - Unauth Acts Intent to Impair Access			
Suspect Not ID Victim Unsupportive			1
Computer - Use Intent Secure/Enable Unauth Access			
Unfinalised - Undetected		1	
Computer - Use with Intent Secure Unauth Access			
Caution - Adults	3		
Charged/Summoned	1		
Investigation Complete No Suspect	2		
Named Suspect Evidential Difficulties	1		
Named Suspect Victim Unsupportive		1	
Suspect Not ID Victim Unsupportive	1		
Unfinalised - Undetected		1	1
Fraud - Unauthorised Access to Computer Material			
Charged/Summoned	1		
Investigation Complete No Suspect	3		
Named Suspect Victim Unsupportive	1		
Fraud - Unauthorised modification of Computer Material			
Investigation Complete No Suspect	1		
Unfinalised - Undetected	1		
Total	22	7	2

Of the Crimes above those which referenced the terms: Hacking / Smart Device / Connected Device
(of these only "Hacking" is recorded)

Offence by Outcome	2015	2016	2017
Computer - Unauth Access Facilitate Offence Investigation Complete No Suspect	2		
Computer - Unauth Access to Material with Intent Charged/Summonsed	1		
Computer - Unauth Acts Intent to Impair Access Suspect Not ID Victim Unsupportive			1 1
Computer - Use with Intent Secure Unauth Access Investigation Complete No Suspect Named Suspect Evidential Difficulties Suspect Not ID Victim Unsupportive	1 1 1		
Fraud - Unauthorised Access to Computer Material Investigation Complete No Suspect	2		
Fraud - Unauthorised modification of Computer Material Investigation Complete No Suspect	1 1		
Total	9	7	1

Leicester Police Force

Incidents

Financial Year:	Call Type:	Description
2016/2017	Crime Related Incident	HACK ON SCHOOL WEB
2017/2018	Contact Record	THREATS TO HACK WEBSITE

Crimes

Financial Year:	Stats Classification Desc	Type:	Investigation Outcome:

2016/2017	Articles connected with computer misuse	Unauthorised access to personal email account.	15: Police - named suspect, victim supports but evidential difficulties
2016/2017	Articles connected with computer misuse	Hacking of company website	18: Investigation complete no suspect identified
2016/2017	Articles connected with computer misuse	Unauthorised access to company email account	15: Police - named suspect, victim supports but evidential difficulties
2016/2017	Articles connected with computer misuse	Hacking/Unauthorised access to medical records and internal systems.	18: Investigation complete no suspect identified
2016/2017	Articles connected with computer misuse	Unauthorised Access to company account	14: Victim declines/unable to support action to identify offender
2016/2017	Articles connected with computer misuse	Unauthorised Access to computer	1: Summoned/postal requisition
2016/2017	Articles connected with computer misuse	Unauthorised Access to case file	1: Charged
2016/2017	Articles connected with computer misuse	Unauthorised access to Twitter account.	18: Investigation complete no suspect identified
2016/2017	Articles connected with computer misuse	Unauthorised access to icloud account	8: Community resolution
2016/2017	Articles connected with computer misuse	Hack/unauthorised access of email account	15: Police - named suspect, victim supports but evidential difficulties
2016/2017	Articles connected with	Unauthorised access to gmail account	16: Victim declines/withdraws support - named suspect identified

	computer misuse		
2016/2017	Articles connected with computer misuse	Hacking of laptop	15: Police - named suspect, victim supports but evidential difficulties
2016/2017	Articles connected with computer misuse	Hacking of school computer systems	18: Investigation complete no suspect identified
2016/2017	Articles connected with computer misuse	Company website hacked	18: Investigation complete no suspect identified
2016/2017	Articles connected with computer misuse	Unauthorised access to company syste,account	3: Adult caution
2016/2017	Articles connected with computer misuse	Hacking/Unauthorised access of social media and email accounts	18: Investigation complete no suspect identified
2016/2017	Articles connected with computer misuse	Hacking of school website, by a suspect named ISIS	18: Investigation complete no suspect identified
2016/2017	Articles connected with computer misuse	Hack/Unauthorised access to Instagram account, and changing username/password.	15: Police - named suspect, victim supports but evidential difficulties
2017/2018	Articles connected with computer misuse	Unauthorised access to icloud account	16: Victim declines/withdraws support - named suspect identified
2017/2018	Articles connected with computer misuse	Unknown suspect has hacked into victims email account and posted photographs of emails through his girlfriends postbox.	18: Investigation complete no suspect identified
2017/2018	Articles connected with computer misuse	Unknown person has created a clone facebook account.	18: Investigation complete no suspect identified

2017/2018	Articles connected with computer misuse	Unknown person has gained unauthorised access to company's trading site and made alterations.	14: Victim declines/unable to support action to identify offender
2017/2018	Articles connected with computer misuse	Schoolchild gives her Instagram password out to friends, inappropriate messages are then sent from her account shortly after.	18: Investigation complete no suspect identified
2017/2018	Articles connected with computer misuse	Hacking of CCTV system preventing remote access.	18: Investigation complete no suspect identified
2017/2018	Articles connected with computer misuse	Unauthorized access to Facebook account and printing photos off	18: Investigation complete no suspect identified
2017/2018	Articles connected with computer misuse	Unauthorized access to iCloud account	14: Victim declines/unable to support action to identify offender
2017/2018	Articles connected with computer misuse	Unauthorized access to Facebook account	15: Police - named suspect, victim supports but evidential difficulties
2017/2018	Articles connected with computer misuse	Unauthorized access to online personal accounts	15: Police - named suspect, victim supports but evidential difficulties
2017/2018	Articles connected with computer misuse	Unauthorized access to Instagram account	18: Investigation complete no suspect identified
2017/2018	Articles connected with computer misuse	Advertising DDOS attack service	18: Investigation complete no suspect identified
2017/2018	Articles connected with computer misuse	Unauthorized access to Facebook.	18: Investigation complete no suspect identified
2017/2018	Articles connected with	Unauthorized access to Facebook account.	18: Investigation complete no suspect identified

	computer misuse		
2017/2018	Articles connected with computer misuse	Unauthorised access to CCTV system	18: Investigation complete no suspect identified
2017/2018	Articles connected with computer misuse	Unauthorised sending of work emails to personal email account.	15: CPS - named suspect, victim supports but evidential difficulties
2017/2018	Articles connected with computer misuse	Victim believes his snapchat account has been hacked	18: Investigation complete no suspect identified
2017/2018	Articles connected with computer misuse	Unauthorised access to Snapchat account.	16: Victim declines/withdraws support - named suspect identified
2017/2018	Articles connected with computer misuse	Unauthorised access to HMRC account	18: Investigation complete no suspect identified

Merseyside

RESPONSE

The below data relates to offences under the Computer Misuse act 1990.

2015 – 2016 – One case, 2016 – 2017 – Six cases.

Year	Description as reported
2015 – 2016	Unknown offender has accessed a school e-mail account and closed it down, without authority.
2017 - 2018	On a mobile phone, gained access to Facebook account and sent abusive messages.
Ditto	Allegation that refund due because of slow internet, received by unsolicited telephone call. Apparent unauthorised access to computer blocking action, following unsuccessful telephone call, in which no bank details passed.

Ditto	Unauthorised access to cloud storage and then contact with person on contact list.
Ditto	Unauthorised access to e-mail and social media accounts.
Ditto	Unauthorised access to computer and installation of a (DDOS) distributed denial of service programme which caused computer to crash. Admitted when challenged by relevant staff.
Ditto	Under ages children have been sharing indecent images – some have been hacked and shared without permission.

Norfolk and Suffolk

Financial Year 2016/17

5 crimes have been recorded during 2016/17; all of which were recorded by Suffolk Constabulary.

HO Class Crime Text 053/34 Exempt Section 31 053/35 Exempt Section 31

053/35 During hours of darkness in rural market town unknown person has instigated a virus in private business server which has encrypted personal data files which can only be accessed by the users by paying a ransom of 1087 Bitcoins

053/35 During hours of darkness unknown person has deployed ransomware virus onto private business server which has encrypted numerous files

053/35 During a 3 day period town centre industrial estate unknown person has gained unauthorised access to a private business server by unknown means, causing all of the data files to be locked. Suspect is demanding a Bitcoin payment of 5 BC in return for the files.

Financial Year 2016/17

1 crime has been recorded, which was recorded by Norfolk Constabulary.

HO Class Crime Text 053/35 Exempt Section 31

North Wales

Home Office Description	Status	Fiscal Year	Summary
Unauthorised computer access with intent to commit other offences (recordable)	Cancel/transfer crime	2016	Action fraud report received stating that two computer servers have been hacked.
Cause a computer to perform function to secure / enable unauthorised access to a program / data (recordable)	Cancel/transfer crime	2016	Unknown offenders have gained access to the ip's website and have placed things on website
Unauthorised acts with intent to impair operation of or prevent / hinder access to a computer (recordable)	Victim supports/ evidential difficulties - Named suspect identified	2016	DP arrested for offences under the Computer Misuse Act.
Cause a computer to perform function to secure / enable unauthorised access to a program / data (recordable)	New	2017	Known Offender has accessed the computer network of the Aggrieved business and deleted data and access logs following his dismissal from working for the Aggrieved.

Northumbria

Between 12th march 2012 and 14th july 2015; cause computer to perform a function with intent to secure unauthorised confidential information

Caller reporting that website was hacked into

Cause denial of service attack against computer servers with the intent to impair the operation of computer

Succumbs to malware infection of computers which locks files requiring payment to release same

Telephony system hacked into and the have dialled premium rate international telephone numbers costing the victim money.

Send payment for veh; later discover account is hacked and payment sent to wrong account

Email sent demanding money for work to be carried out;email account had been hacked into

Person hacked into the victims social media account and sent messages to social media account; causing problems

Known offender accesses ips facebook account sends messages to other parties purporting to be ip of harassing/ abusive nature.

Hack into facebook account and private messa ges victim; impersonating friend. Offender contacts victim and persuades them to obtain 3 mobile phone contracts or payment. Victim

meets offender and hands over phones. Offender leaves with phones. Victim does not receive any payment.

Following contact on a hacked facebook account; ip is induced to take out mobile phone contracts by u/k person/s who offer money for phones; no money received when phones handed over

Employee uses company passwords to access data on the company computer system and obtain the data without permission

Order building materials online- hacker send fraudulent email to ip requesting ip pay half payment for goods upfront ip pay via bank transfer then later realise the fraud

Ip receive ransomware pop up warning message on computer stating they have to purchase 4 bit coins to receive a decryption key.

Ip reports iphone has been hacked

Person has changed the password on ip's booking account

Ip's ex-partner attempts to 'hack' ip's facebook account

Hacks ip's social media accounts and changes security details

Ip's website has been hacked

Access victim's facebook account illegally by entering password to obtain personal information about the ip.

use unknown means to access private facebook account

Offender causes a computer to perform a function within intent to secure unauthorised access to data held on the computer for own purposes

I would like to know the number of reported crimes of hacking from members of the public over the last two financial years.

Mo

Freedom of information act 2000 (foia) request 512/18 - hacking

Opens an email that contained a virus which has denied access to the records stored on the computer; suspect has demanded a \$3000 ransom before the files would be restored

Person access ip's facebook and email accounts using password; whilst on computer change password preventing the ip to access email and facebook accounts

Access computer whilst employed

Accesses website - accesses data and information that was restricted; no damage caused; eventually stops.

Hacks into ip's email account removing emails and documents from account

use computer to access personal account - gaining information from account and changing password without permission of the ip

stolen contact information to use in new role with another company

Hacks into email account and accesses social media (instagram)- thereafter alters information within and posts false and embarrassing threads in the name of victim causing harassment

Hacks into email account of victim and accesses social media of victim (snapchat) thereafter alters information within and posts false and embarrassing threads in the name of victim causing harassment

Hacks into email account of victim and accesses social media of victim (x3). Thereafter alters information within and posts false and embarrassing threads in the name of victim; causing harassment

Hacks facebook account changing password details

Obtained details of victims email address send and post various parts of personal emails onto social media and other formats

Hack into email accounts and request change to bank details.

Hack into accounts and post content online. Including posting a photo of the ip on a website

Hack into email account and send email to transfer funds from the victims account into the offenders own account. Steal money

Uses computer system to access ips twitter account and steal thereby denying access

Uses victim's mobile phone to access twitter account and post a derogatory comment on twitter feed without consent.

Hack into facebook account and impersonating one of her friends; persuade ip to take out 3 mobile phone contracts with a view to handing over the handsets. Ip arranges to meet friend ; but on arrival no sign of friend;

Access facebook account and change password and email address to prevent access.

Accessed computer system and obtained the details of customers.

Access computer systems in order to retrieve the personal and financial details

Hack facebook account; changed settings;

Uses victims details to access phone and locks iphone

Telephone system has been hacked.

Email account hacked and has sent invoices requesting payments are directed to an alternative bank account

Telephony system hacked by u/k suspects who have made premium rate calls world wide resulting in financial loss to the victim

Attacked by a ransom ware virus; - files have been encrypted.

Accesses data on computer; opening messages intended ; offender threatens to hack any new accounts

U/k person places virus into company computer by u/k menas;demands fee to fix

Change password of ip account; then sends pictures from ip account;

Access internet system; create malicious account and uses to change wifi settings;

Uses ransomware to disable computer network and then threaten with disposal of files unless payment made

Hacks into facebook account advertising money making scheme. I p responds to advert and follows instructions to buy mobile phone contracts and hand phones over to for money the ip does not receive

Hack email account and ask ip to pay funds into an account which had incorrect supplier details.

Call to ip reporting rtc; request member of staff calls him back via conference call. Request details from males but line cuts out. Unable to recontact. Information received from fraud activation software that lines have remained open and hacked and further phone calls have been made on the companies lines.

Hack facebook account and contact ip offering employment;

access computer system via mobile device using internet and deletes files

Access computer system and sends fake emails ; requesting that all payments be sent to a different account

Hack into website; changing settings and rendering forwarding link inoperable.

Hacks ips friends facebook account offering money as part of a business opportunity. Ip replies showing interest and offender directs ip to take out 4 mobile phone contracts in return for money. Ip meets offenders brother and hands him the phone with a promise payment would be made to the ips bank account. No payment received

Uk person have hacked phone lines during period of time

Hacks into facebook account advertising money making scheme. Victim responds to advert and follows instructions to buy 8 mobile phone contracts and hands over to an u/k male for money for which the victim does not receive

Access facebook account of ip - changes made to the account including telephone and password details facebook contact ip to alert of the changes

Attempt to access ips mobile phone account with ee without consent.

Hacks facebook account offering money and cheap phone contracts as part of business opportunity. Ip replies showing interest and offender directs ip to take out 2 mobile phone contracts in return for money and cheap phone contract

Person has gained access to ips facebook account and changed the login details

person secures unauthorised access to ips facebook account and posts series of defamatory messages about ip.

Hacked into telephony system making multiple international premium rate calls for extended periods of time that has caused loss to the victim.

Computer system has been infected with ransomware. This has denied access to business files

Gains remote unauthorised access to ip's computer with intent to commit fraud

hacks facebook account; offering money as part of business opportunity; ip replies showing interest; offender direct ip to take out 4 mobile phone contracts and instruct ip to hand over phones and contracts to offenders brother; ip does so expecting money to be forwarded to his account; but this fails to happen.

Hack into skype account causing fraudulent transactions to be made by expired debit card
Access ip's personal email account

Access to server hosting ips website using vulnerablity in word press. Once access gained offender modifys website content rendering website inoperable.

Hack a facebook account and make cont act with the victim. The victim supplies personal data ils to the hacked facebook account on the promise of legitimate work. Victim purchase four mobile phone contracts hand phones to offender and never receive payment.

Access twitter account and e-mails accounts of company and post inappropriate images and comments with the intention of committing fraud.

instigate ddos attack on computer system. The attack takes the computer system off line for a couple of hours

Hacks into computer system and server; deletes history then recreates new history; change permissions on files and reboots system.

Access facebook account; under a false competition request allowing access to al private information including friends; hacker then distrubute indecent images to people on the list.

Hacked telephone system making international premium rate calls causing loss to the ip and gain to the offender.

Victim has had her business website hacked; causing her to lose business.

Hacked into online banking and transfered #3;500 to account and made payments;

Offender has hacked into laptop. A page has appeared saying x2 people were watching and has x 2 viruses on computer

Unknown persons are intentionally hacking into personal computer and other devices compromising said devices

Received an email into account and upon opening it unzipped a file containing a virus - the virus distributor then made a bitcoin demand for the key.

Email account has been hacked and a message has been sent asking him to transfer money. Resulting in financial loss.

Facebook account hacked.

Access facebook account. Read messenger.

Computer displays a message saying there was an encryption virus on the system. Message was closed; however the computer then started playing up approx 1 hour later. Suspects were looking for approx 5000 in bit coins.

Scotland

2016/17 2017/18

Recorded	17	32
Detected	8	6

West Mercia and Warwickshire

West Mercia Police 9689:

Incident Type	2016/17	2017/18	Total
AS NUISANCE	6	13	19
AS PERSONAL	8	9	17
CR ASSAULTS	3	2	5
CR BURG RESIDENTIAL		1	1
CR BURGLARY DWELLING	1		1
CR BURGLARY OTHER	1		1
CR CRIMINAL DAMAGE	1	2	3
CR DECEPTION/FRAUD/FORGERY	2	7	9
CR HARASSMENT/STALKING	4	2	6
CR OTHER FORCE / AGENCY	2	4	6
CR OTHER UNLISTED	6	3	9
CR THEFT OTHER	1	1	2
CR THREATS TO KILL	1		1
PS ABSCONDER/AWOL/BAIL	1		1
PS CIVIL DISPUTE	3	1	4
PS CONCERN FOR SAFETY	11	16	27
PS DOMESTIC INCIDENT	7	21	28
PS MISSING PERSON		2	2
PS SUDDEN-UNEXPLAINED DEATH		1	1
PS SUSP CIRCUMSTANCES	17	7	24
Grand Total	75	92	167

Warwickshire Police 00427:

Incident Type	2016/17	2017/18	Total
Burglary Dwelling	1		1
Concern for Safety	17	7	24
Domestic incident	8	11	19
Fraud and Forgery	1	3	4
Harassment/Stalking		5	5
Hoax Call		1	1
Other crime	9	4	13

Other Force/Agency		1	1
Personal	2	3	5
Sexual Offence		3	3
Suspicious circumstances/Insecure premises or vehicles	5	4	9
Theft (not vehicle related)	1	1	2
Violence	4		4
Grand Total	48	43	91

West Midlands

2016/17	FINAL CLASSIFICATION	
	ADMIN	30
	ANTI SOCIAL BEHAVIOUR	4
	FIRST CONT RSLN	24
	MISCELLANEOUS	1
	NON INCIDENT	12
	PUBLIC SAFETY/WELFARE	166
	RECORDED CRIME	40
	TOTAL	277
2017/18	FINAL CLASSIFICATION	
	ADMIN	40
	ANTI SOCIAL BEHAVIOUR	9
	FIRST CONT RSLN	6
	NON INCIDENT	6
	PUBLIC SAFETY/WELFARE	207
	RECORDED CRIME	61
	TOTAL	329