Details

Queensland Police Service

Report no.:	QP1500149635
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	29/01/2015 06:26 - 30/01/2015 14:00
Reported time:	30/01/2015 18:30
Place of offence:	Sch4p4(6) (Patrol group: RIVERSIDE, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: SOUTH BRISBANE, Division: WEST END, Stats area: 305011525)
Clearance status:	Finalised
Summary:	Hacking / Misuse - Cyber [0761] ; Sch4p4(6)
Concluded summary:	

Printed: 07/08/2017 10:01 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Patrol group: RIVERSIDE, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: SOUTH BRISBANE, Division: WEST END, Stats area: 305011525) (Land li] / [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: RIVERSIDE, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: SOUTH BRISBANE, Division: WEST END, Stats area: 305011607)), Id Sch4p4(6) :] / Status: [Arrested (1a)]
   Cleared Unit: [#4026074 CAFFERY, B.] / [03/02/2015]

Modus operandi:

1. Location: Commercial. Subtype: Office. Other behavior at scene: Other. Method of escape: Unknown. No. of offenders/suspects: One. Free text keywords: AT 0726 HOURS ON 29/01/2015, THE SUSPECT ATTEMPTED TO LOG IN FROM AN UNKNOWN IP ADDRESS TO THE Sch4p4(6) FILE DATABASE USING Sc OLD USERNAME AND PASSWORD [Sch4p4(6) HOWEVER THE LOGIN FAILED. AT 0726 HOURS ON 29/01/2015, THE SUSPECT USED THE USERNAME Sch4p4(AND PASSWORD Sch4p4(6) WHICH SUCCESSFULLY LOGGED THE SUSPECT ONTO THE DATABASE. THE USERNAME AND PASSWORD BELONGS TO Sch4p4(, THE CHIEF OPERATING OFFICER OF Sch4p4(6) . BETWEEN THE NOMINATED OFFENCE TIMES, THE SUSPECT HAS LOGGED ON NUMEROUS TIMES, AND HAS ACCESSED SECURE AND CONFIDENTIAL INFORMATION BELONGING TO Sch4p4(6) Sch4p INCLUDING BUT NOT LIMITED TO NEWSLETTERS, EMPLOYEE PAYSLIPS, FINANCIAL LEDGERS, WORKFORCE PLANNING INFORMATION, EMPLOYEE PACKAGES AND SALARIES, BUSINESS PLANNING DATA, BROAD PAPERS, COMPANY PERFORMANCE STRATEGY DOCUMENTS, EMAILS, FAMILY TRUST DOCUMENTS FOR Sch4p4(6) , EMPLOYEE BONUS INFORMATION, AND SAFETY INVESTIGATION REPORTS. AT APPROXIMATELY MIDDAY ON THE 29/01/2015, THE SUSPECT CONTACTED EMPLOYEE Sch4p4(6) BY TELEPHONE AND STATED WORDS TO THE EFFECT OF “I HAVE A LIST OF PEOPLE WHO ARE GOING TO BE MADE REDUNDANT, AND YOU ARE ON IT. AT AN UNKNOWN TIME, THE SUSPECT FORWARDED Sch4p4(6) DOCUMENTS TO AN EX-EMPLOYEE, Sch4p4(6) , TO HER PERSONAL EMAIL, FROM THE SUSPECT’S PERSONAL EMAIL (EMAIL ADDRESS UNKNOWN AT THIS TIME). THE SUSPECT HAS CONTACTED AND UNKNOWN QUANTITY OF Sch4p4(6) EMPLOYEES REGARDING INFORMATION HE HAS OBTAINED. GENERAL REPORT THE VICTIM BUSINESS IS A Sch4p4(6) SERVICES COMPANY. THE SUSPECT IS A PREVIOUS EMPLOYEE OF THE COMPANY, WHO WAS SUBJECT OF A FORCED REDUNDANCY ON THE Sch4p4(6) . THE COMPANY HAS BEEN SUFFERING

PROFIT LOSSES AND OVER SEVERAL MONTHS HAVE HAD TO MAKE SIGNIFICANT JOB CUTS OF APPROXIMATELY 400 EMPLOYEES, WHICH THE SUSPECT IS ONE OF. THE SUSPECT HAS CAUSED ISSUES FOR THE VICTIM COMPANY SINCE HIS REDUNDANCY. WITNESS Sch4p4(6) WAS INVOLVED IN THE SUSPECT'S REDUNDANCY AND IT IS HIS USERNAME AND PASSWORD THAT WAS USED BY THE SUSPECT. Sch4p4 HAS BEEN EMPLOYED BY THE COMPANY FOR 2 YEARS, AND HAD NEVER CHANGED HIS TEMPORARY PASSWORD, WHICH IS Sch4p4(6) , WHICH WAS PROVIDED BY THE COMPANY. THE INFORMANT HAS CONTACTED Sch4p4 TO VERIFY WHETHER THE DOCUMENTS WERE ACCESSED BY HIM, AND WAS ADVISED THAT DURING THE OFFENCE TIMES, Sch4p4 WAS COMMUTING VIA PLANE FROM Sch4p4(6) AND BACK. THE COMPANY HAS NOW Sch4p4(6) LOGIN AND WILL PROVIDE THIS INFORMATION TO POLICE IF IT BECOMES AVAILABLE. THE INFORMANT IS MAKING ATTEMPTS TO IDENTIFY ALL EMPLOYEES CONTACTED BY THE SUSPECT. THE INFORMANT BELIEVES THAT QUITE A LARGE NUMBER OF EMPLOYEES HAVE BEEN CONTACTED REGARDING THEIR REDUNDANCIES AS THERE HAS BEEN SIGNIFICANT UNREST BETWEEN EMPLOYEES SINCE THE INCIDENT OCCURRED. THE INFORMANT PROVIDED AN AUDIT REPORT AND A SECURITY AUDITING REPORT WHICH HAVE BEEN SCANNED AND UPLOADED TO THE OCCURRENCE. THE INFORMANT WILL ATTEMPT TO OBTAIN AN INJUNCTION THAT PREVENTS THE SUSPECT FROM DISCLOSING INFORMATION TO OTHER PARTIES OR BUSINESSES. SOC NOT REQUIRED. WITNESSES NOMINATED. Sch4p4(6) .

Reports:

General report

Occurrence: QP1500149635 Hacking / Misuse - Cyber [0761] @30/01/2015 18:30 (Sch4p4(6) (Patrol group: RIVERSIDE, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: SOUTH BRISBANE, Division: WEST END, Stats area: 3

Task: T1500381580 [Init rpt - Closed] Due: 31/01/2015 20:18 #4032464 ROBINSON, E. ->#4032464 ROBINSON, E. [Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1500149635 Hacking / Misuse - Cyber [0761] @30/01/2015 18:30 Sch4p4(6)

Author: #4024982 HUGHES, J.

Report time: 30/01/2015 18:30

Entered by: #4032464 ROBINSON, E.

Entered time: 30/01/2015 20:29

Remarks: Steal as a clerk or servant [0750] ; Sch4p4(6)

Narrative:

MO

At 0726 hours on 29/01/2015, the suspect attempted to log in from an unknown IP address to the Sch4p File Database using S old username and password [Sch4p4(6 however the login failed. At 0726 hours on 29/01/2015, the suspect used the username Sch4p4(and password Sch4 S which successfully logged the suspect onto the database. The username and password belongs to Sch4p4(6) , the Chief Operating officer of Sch4p4(6) . Between the nominated offence times, the suspect has logged on numerous times, and has accessed secure and confidential information belonging to Sch4p4(6) , including but not limited to newsletters, employee payslips, financial ledgers, workforce planning information, employee packages and salaries, business planning data, broad papers, company performance strategy documents, emails, family trust documents for Sch4p4(6) , employee bonus information, and safety investigation reports. At approximately midday on the 29/01/2015, the suspect contacted employee Sch4 Sch4p4(6) by telephone and stated words to the effect of "I have a list of people who are going to be made redundant, and you are on it. At an unknown time, the suspect forwarded Sch4p4(6) documents to an ex-employee, Sch4p4(6) , to her personal email, from the suspect's personal email (email address unknown at this time). The suspect has contacted and unknown quantity of Sch4p4(6) employees regarding information he has obtained.

GENERAL REPORT

The victim business is a Sch4p4(6) s services company. The suspect is a previous

employee of the company, who was subject of a forced redundancy on the Sch4p4(S. The company has been suffering profit losses and over several months have had to make significant job cuts of approximately 400 employees, which the suspect is one of. The suspect has caused issues for the victim company since his redundancy. Witness Sch4p4(6) was involved in the suspect's redundancy and it is his username and password that was used by the suspect. Sch4p has been employed by the company for 2 years, and had never changed his temporary password, which is Sch4p4(, which was provided by the company. The informant has contacted Sch4p to verify whether the documents were accessed by him, and was advised that during the offence times, Sch4p was commuting via plane from Sch4p4(6) and back. The company has now Sch4p4(6) ll provide this information to Police if it becomes available. The informant is making attempts to identify all employees contacted by the suspect. The informant believes that quite a large number of employees have been contacted regarding their redundancies as there has been significant unrest between employees since the incident occurred. The informant provided an audit report and a security auditing report which have been scanned and uploaded to the occurrence. The informant will attempt to obtain an injunction that prevents the suspect from disclosing information to other parties or businesses. SOC not required. Witnesses nominated. Sch4p4(6)

Details

Queensland Police Service

Report no.:	QP1500305428
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	26/02/2015 20:23 - 26/02/2015 20:44
Reported time:	02/03/2015 10:00
Place of offence:	Sch4p4(6) Patrol group: GOLD COAST ENTERTAINMENT PRECINCT, Court Dist./Div.: GOLD COAST, Region: SOUTH EASTERN, District: GOLD COAST, Division: BROADBEACH, Stats area: 307103515, Beat:
Clearance status:	Finalised
Summary:	Hacking / Misuse - Cyber - Sch4p4(6)
Concluded summary:	

Printed: 06/08/2017 21:23 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Patrol group: GOLD COAST ENTERTAINMENT PRECINCT, Court Dist./Div.: GOLD COAST, Region: SOUTH EASTERN, District: GOLD] / [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: GOLD COAST NORTHERN, Court Dist./Div.: GOLD COAST, Region: SOUTH EASTERN, District: GOLD COAST, Division: NERANG, Stats area: 307153525)), Id #:Sch4 / Status: [Notice to appear (1b)]
   Cleared Unit: [NERANG STATION (32 COTTON ST, NERANG, QLD Australia 4211 (Court Dist./Div.: GOLD COAST, Region: SOUTH EASTERN, District: GOLD COAST, Division: NERANG, Stats area: 307153567))] / [23/09/2015]

Modus operandi:

1. Location: Commercial. Subtype: Pharmacy. Other behavior at scene: Other. Method of escape: Other. No. of offenders/suspects: One. Free text keywords: THE NOMINATED SUSPECT WAS AN EMPLOYEE OF THE VICTIM COMPANY, BEING Sch4p4(6) BETWEEN DECEMBER 2013 UNTIL HE RESIGNED ON THE Sch4p4(6) . THE NOMINATED SUSPECT HAS LEFT THE BUSINESS TO BEGIN A COMPETITION COMPANY, CALLED Sc Sch4p4(6) WHICH SELLS PHARMACEUTICAL GOODS AND MEDICATIONS. WHILST EMPLOYED AT Sch4p4(6) HE WAS A PHARMACIST AND HAD ACCESS TO THE Sch4p4(6) COMPUTER PROGRAMMED CALLED Sch4p4(6) WHICH WAS A DATABASE THAT KEPT ALL TRANSACTIONS OF CUSTOMER DETAILS AND GOODS PURCHASED. ON THE 22/02/2015 THE INFORMANT WAS WORKING AT Sch4p4(6) Sch4p4(6) WHEN HE HAS NOTICED ONE OF THE COMPUTER SCREEN ICONS WAS BEING MOVED REMOTELY. IT IS BELIEVED THE NOMINATED SUSPECT AS ATTEMPTED TO GAIN ACCESS TO THE Sch4p4(6) DATABASE TO OBTAIN CUSTOMER INFORMATION TO SOURCE HIS OWN BUSINESS AT Sch4p4(6) ..

Reports:

General report

Occurrence: QP1500305428 Hacking / Misuse - Cyber [0761]

	@02/03/2015 10:00 Sch4p4(6) (Patrol group: GOLD COAST ENTERTAINMENT PRECINCT, Court Dist./Div.: GOLD COAST, Region: SOUTH EASTERN, District:
Task:	T1500787269 [Init rpt - Closed] Due: 03/03/2015 14:03 #4029291 WEIR, S. ->#4029291 WEIR, S. [Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1500305428 Hacking / Misuse - Cyber [0761] @02/03/2015 10:00 (Sch4p4(6)
Author:	#4029291 WEIR, S.
Report time:	02/03/2015 10:00
Entered by:	#4029291 WEIR, S.
Entered time:	02/03/2015 14:09
Remarks:	Hacking / Misuse - Cyber - Sch4p4(6)

Narrative:

MO:

The nominated suspect was an employee of the victim company, being Sch4p4(6) between December 2013 until he resigned on the Sch4p4(6) . The nominated suspect has left the business to begin a competition company, called Sch4p4(6) which sells pharmaceutical goods and medications. Whilst employed at Sch4p4 he was a pharmacist and had access to the Sch4p4 computer programmed called Sch4p4(which was a database that kept all transactions of customer details and goods purchased. On the 22/02/2015 the informant was working at Sch4p4(6) when he has noticed one of the computer screen icons was being moved remotely. It is believed the nominated suspect as attempted to gain access to the Sch4p4 database to obtain customer information to source his own business at Sch4p4(6) .

GENERAL REPORT:

Police attended Sch4p4 and spoke with the informant Sch who stated he was the person who was working at the time when he observed the Sch4p4 computer being accessed remotely and has unplugged this computer to stop any further access and has then run a log in programme to attempt to find out who has gained entry to the Sch4p4(programme. A copy of the access log has been scanned into this report, being highlighted by the informant to show where access has been gained which is believed to be the ex-employee Sch4p4(The log in shows access remotely gained at 2023 hours 26/02/2015 via participant Sch4p4(6) . The informant states Sch4p4(6) nickname from work was Sch At this time the log shows that "Sch4 has changed the password to enter the Sch4p4(programme and then at 2027 hours a number of files had been attempted to be copied. It is believed these files would have contained customer details and he medications sold to these customers. A second attempt to copy files was again made at 2035 hours, then at 2044 hours the informant has disconnected the server. Police have obtained details of the ex-employee Sch4p4(and he has since been listed as WFQ regarding this matter. Informant believes that Sch4p4(6) has attempted to gain access to these files to gain a benefit for his business by having Sch4p4(customer database. SOC not required.

Details

Queensland Police Service

Report no.:	QP1500604183
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	01/01/2011 00:01 - 01/05/2015 13:00
Reported time:	01/05/2015 13:00
Place of offence:	SUBURB - BADU ISLAND, BADU ISLAND, QLD Australia 4875 (Patrol group: TORRES STRAIT, Court Dist./Div.: THURSDAY ISLAND, Region: NORTHERN, District: FAR NORTH, Division: BADU ISLAND, Stats area: 350106963)
Clearance status:	Finalised
Summary:	Hacking / Misuse - Cyber [0761]; Suburb of Badu Island; Victim - Sch4p4(6) Sch4p4S ; Suspect - Sch4p4(6)
Concluded summary:	

Printed: 06/08/2017 21:13 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) Patrol group: TORRES STRAIT, Court Dist./Div.: THURSDAY ISLAND, Region: NORTHERN, District: FAR NORTH, Division: BADU ISLAND, Stats area: 350106963)), Id #:22780] / [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: CAIRNS COUNTRY, Court Dist./Div.: CAIRNS, Region: NORTHERN, District: FAR NORTH, Division: EDMONTON, Stats area: 350052074, Beat: WHITE ROCK)), Id #:10130] / Status: [Warrant issued (1e)]
   Cleared Unit: [THURSDAY ISLAND CIB (160 DOUGLAS ST, THURSDAY ISLAND, QLD Australia 4875 (Court Dist./Div.: THURSDAY ISLAND, Region: NORTHERN, District: FAR NORTH, Division: THURSDAY ISLAND, Stats area: 350106950))] / [16/12/2015]

Modus operandi:

1. Location: Dwelling. Subtype: House. Location specific: Unknown. Occupancy: Not known. Victim age: Female elderly (over 65). Victim's prior actions: Unknown. Victim injuries sustained: No injury. Relationship to offender: Parent of offender. Theft acts: Selective search. Other behavior at scene: Unknown. Method of escape: Unknown. No. of offenders/suspects: One. Computer hacking method: Access/interfere data. Communication device: Other. Free text keywords: BETWEEN THE OCCURRENCE DATES THE SUSPECT WAS THE VICTIM'S PRIMARY CARER WITH ACCESS TO HER BANK ACCOUNTS PRIMARILY IN THE FORM OF INTERNET BANKING. THE SUSPECT HAS DURING THE OFFENCE PERIOD REMOVED THE VICTIM'S PENSION FOR PURPOSES NOT RELATING TO THE VICTIM. FOR THE YEAR OF 2014 IT IS BELIEVED THE SUSPECT HAS REMOVED $11000. .

Reports:

General report

Occurrence:	QP1500604183 Hacking / Misuse - Cyber [0761] @01/05/2015 13:00 (SUBURB - BADU ISLAND, BADU ISLAND, QLD Australia 4875 (Patrol group: TORRES STRAIT, Court Dist./Div.: THURSDAY ISLAND, Region: NORTHERN, District: FAR NORTH, Division: BADU ISLAND, Stats area
Task:	T1501576111 [Init rpt - Closed] Due: 02/05/2015 14:03

#4028333 FINDLATER, F. ->#4028333 FINDLATER, F. [Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1500604183 Hacking / Misuse - Cyber [0761] @01/05/2015 13:00 (SUBURB - BADU I

Author: #4029165 FOWLES, J.
Report time: 01/05/2015 13:00
Entered by: #4028333 FINDLATER, F.
Entered time: 01/05/2015 14:06
Remarks: Hacking / Misuse - Cyber [0761]; Suburb of Badu Island; Victim - Sch4p4(6) ; Suspect - Sch4p 4(6)

Narrative:
MO

Between the occurrence dates the suspect was the victim's primary carer with access to her bank accounts primarily in the form of Internet banking. The suspect has during the offence period removed the victim's pension for purposes not relating to the victim. For the year of 2014 it is believed the suspect has removed $11000.

GENERAL REPORT

At the reported time QATSIP officer has contacted Thursday Island police and advised of the offence. No person has access to the bank account other than the suspect. Suspect not flagged pending investigation. Further enquiries still to be conducted. Police are unable to speak to the informant due to her being hearing impaired. Communication to date has been through Sch4p4(6) . Request that this matter be sent to Thursday Island CIB for their attention. No witnesses. SOC not required. No CCTV. No Insurance.

Details

Queensland Police Service

Report no.:	QP1500729211
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	19/04/2015 00:01 - 21/05/2015 23:59
Reported time:	26/05/2015 15:47
Place of offence:	Sch4p4(6) (Patrol group: RIVERSIDE, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: SOUTH BRISBANE, Division: DUTTON PARK, Stats area: 305011304)
Clearance status:	Finalised
Operation name:	ACORN 1
Misc. file:	Sch4p4(6)
Summary:	Hacking / Misuse - Cyber [0761]; Address - Sch4p4(6) Victim - Sch4p4(6) ; Suspect - Sch4p4(6)
Concluded summary:	

Printed: 06/08/2017 21:35 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Patrol group: EAST GATEWAY, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: HENDRA, Stats area: 305071435, NH] / [Crime: Solved]
   Offender: [Sch4p4(6) (E-mail) Sch4p4(6) , Id #:Sch4p4(6) :Sch4p4(6)] / Status: [Notice to appear (1b)]
   Cleared Unit: [DUTTON PARK STATION (150 ANNERLEY RD, DUTTON PARK, QLD Australia 4102 (Patrol group: RIVERSIDE, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: SOUTH BRISBANE, Division: DUTTON PARK, Stats area: 305011187, NHW: DUTTON PARK 03) (Land line)] / [29/02/2016]

Modus operandi:

1. Sch4p4(6)

L

Sch4p4(6)

Reports:

General report

Occurrence:	QP1500729211 Hacking / Misuse - Cyber [0761] @26/05/2015 15:47 Sch4p4(6) (Patrol group: RIVERSIDE, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: SOUTH BRISBANE, Division: DUTTON P
Task:	T1501910430 [Init rpt - Closed] Due: 27/05/2015 16:50 #4018384 KEYS, G. ->#4018384 KEYS, G. [Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1500729211 Hacking / Misuse - Cyber [0761] @26/05/2015 15:47 (Sch4p4(6)
Author:	#4005267 BIGNELL, S.
Report time:	26/05/2015 15:47
Entered by:	#4018384 KEYS, G.
Entered time:	26/05/2015 16:51
Remarks:	Hacking / Misuse - Cyber [0761]; Address - Sch4p4(6 Victim - Sch4p4(6) , Sch4p4(6) Suspect - Sch4p4(6)

Narrative:

MO

GENERAL REPORT

Date/Time of Export: 26/05/2015 15:42:13

Report ID: ARN-UEGC-ER8A

Cybercrime Type: Cyber Bullying or Stalking

Submitted On: 14/05/2015 16:32:19

Incident Date: 19/04/2015

Offence Module

Select the type of cybercrime that best describes the incident you would like to report: Cyber bullying, sexting, online harassment or stalking

Where did the incident occur?: By email

Is the person who is the subject of this behaviour under 18 years old? : No

Has anyone been told about the incident?: Police

Has the incident involved any inappropriate material or images involving anyone under the age of 18?: No

Has the incident involved the sharing of any inappropriate sexual images without permission?: Yes

Has the incident involved any threats to kill or cause harm?: Yes

Describe the threats which have been made, including when it happened and how many threats were made: unexpect visit to the propriety a day after the threat.Physical assault

---

Victim Module

Why are you reporting this incident?: I am the victim

Has this incident been previously reported to the ACORN, and is the ACORN reference number available?: No

Has any other person, website or agency been informed of the incident?: Yes

Based on the previous response, choose who the incident has been reported to: Website: apple.com

VICTIM 1

Sch4p4(6)

Suspect Module

SUSPECT 1

Suspect Type: Person

Sch4p4(6)

Describe how you got the IP address and why is it linked to the suspect?: Hotmail account was attempted to get access on this day when I was working all day and at the Sch4p4(6) . Suspect, Sch4p ex partner, told me he hacked my accounts and computer 2 weeks after that on the Sch4p4(6) . Showed me pictures of messages of other people's conversation with me on messenger and skype IP registered above is located in Sch4p4

Other additional information about the suspect: Suspect has history of aggressive behaviour recorded on QLD police as domestic violence referral. He lives near my propriety and has showed in the building making me feel unsafe after Sch4p4(6)

Another IP address is recorded in my hotmail account 2 days before this attempt mentioned above.

Sch4p4(6)

SUSPECT 2

Suspect Type: Person

Country: Unknown

Other additional information about the suspect: He also shares in the net sexual activities with group of people without their consent. Some of these participants may be under 18 years of age. All saved in his files on same personal computer.

Method Module

Choose one or more options of where the incident occurred: Email: hotmail, Instant messaging: messenger, Home Computer

Enter the date when the incident occurred on, or the start date if the incident occurred over a period of time: 19/04/2015

Enter the end date if the incident occurred over a period of time: 21/04/2015

Is the incident still ongoing, or behaviour still happening?: No

Sch4p4(6)

.

Is the victim willing to make a formal police statement and attend court in relation to the matter being reported?: Yes

Did anyone else witness the incident?: Yes

Loss Module

Did the incident involve a loss of money, personal information, goods or data?: No

---

Sch4p4(6)

End of answers

Details

Queensland Police Service

Report no.: QP1500844884
Occurrence Type: Hacking / Misuse - Cyber [0761]
Occurrence time: 04/05/2015 00:01 - 19/05/2015 23:59
Reported time: 17/06/2015 21:55
Place of offence: Sch4p4(6) (Patrol group: CITY CENTRAL, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, Stats area: 305011143) (GNAF- Retired as of Feb2010;)
Clearance status: Open
Misc. file: Sch4p4(6)
Summary: Hacking / Misuse - Cyber [0761]. Sch4p4(6). Victim: Sch4p4(6). Suspect: SSch4p4(6)
Concluded summary:

Printed: 06/08/2017 20:49 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Patrol group: CITY CENTRAL, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, Stats area: 305011143) (GNAF- Retired as of Feb2010;))] / [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: IPSWICH COUNTRY, Court Dist./Div.: IPSWICH, Region: SOUTHERN, District: IPSWICH, Division: ROSEWOOD, Stats area: 305253971)), Id #:10457726, :406372277 DL:QLD:01] / Status: [Arrested (1a)]
   Cleared Unit: [HI-TECH CRIME INVESTIGATION UNIT (POLICE - ROMA ST POLICE STATION, ROMA ST, BRISBANE CITY, QLD Australia 4000 (Patrol group: CITY CENTRAL, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, Stats area:] / [30/06/2015]
2. [0551/ Stalking - non Protracted] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Patrol group: BAYSIDE, Court Dist./Div.: BRISBANE/WYNNUM, Region: BRISBANE, District: SOUTH BRISBANE, Division: WYNNUM, Stats area: 305111642) (E-mail) chelle@e] / [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: IPSWICH COUNTRY, Court Dist./Div.: IPSWICH, Region: SOUTHERN, District: IPSWICH, Division: ROSEWOOD, Stats area: 305253971)), Id #:Sch4p4(6) :Sch4p4(6) DL:QLD:01] / Status: [Arrested (1a)]
   Cleared Unit: [HI-TECH CRIME INVESTIGATION UNIT (POLICE - ROMA ST POLICE STATION, ROMA ST, BRISBANE CITY, QLD Australia 4000 (Patrol group: CITY CENTRAL, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, Stats area:] / [30/06/2015]

Modus operandi:

1. Location: Commercial. Subtype: Office. Occupancy: Not known. Other behavior at scene: Other. Method of escape: Unknown. No. of offenders/suspects: One. Computer hacking method: Access/interfere computer systems; Access/interfere data; Access/interfere programs. Free text keywords: OFFENCE MODULE (ARN_6R4X_8YFF) ---------- SELECT THE TYPE OF CYBERCRIME THAT BEST DESCRIBES THE INCIDENT YOU WOULD LIKE TO REPORT: ONLINE IDENTITY THEFT IDENTIFY ONE OR MORE ACCOUNT TYPES WHICH HAVE BEEN COMPROMISED: OTHER: COMPANY

SHARED DROPBOX ACCOUNT DESCRIBE HOW IT BECOME APPARENT THAT THE ACCOUNT(S) HAD BEEN COMPROMISED: VIRUS WAS RELEASED THROUGH OUR COMPANY DROPBOX ACCOUNT VIA A STAFF MEMBERS ACCOUNT. IP ADDRESS IS APPARENT TO HAVE LOGGED IN TO DROPBOX ACCOUNT FROM AN OUTSIDE SOURCE HAS THERE BEEN ANY INDICATION THAT THE COMPROMISED ACCOUNT HAS BEEN USED BY THE SCAMMER?: YES BASED ON THE PREVIOUS RESPONSE, HOW HAS THE ACCOUNT BEEN USED?: TO EMBARRASS OR MISREPRESENT THE ACCOUNT OWNER, SUCH AS ON SOCIAL MEDIA HAS THE BANK OR SERVICE PROVIDER BEEN NOTIFIED ABOUT THE LOST ACCOUNT INFORMATION?: NO METHOD MODULE (ARN_6R4X_8YFF) ---------- CHOOSE ONE OR MORE OPTIONS OF WHERE THE INCIDENT OCCURRED: WORK COMPUTER ENTER THE DATE WHEN THE INCIDENT OCCURRED ON, OR THE START DATE IF THE INCIDENT OCCURRED OVER A PERIOD OF TIME: 19/05/2015 ENTER THE END DATE IF THE INCIDENT OCCURRED OVER A PERIOD OF TIME: 17/06/2015 IS THE INCIDENT STILL ONGOING, OR BEHAVIOUR STILL HAPPENING?: YES IN DETAIL, DESCRIBE THE INCIDENT AND EACH OF THE EVENTS THAT OCCURRED AND WHY YOU BELIEVE THIS IS A CRIMINAL OFFENCE: STAFF SHARE A COMPANY DROPBOX AND ONE OF THE STAFF MEMBERS TARGETED BY 'SUSPECT' NOTICED OUTSIDE LOG-INS ON THEIR COMPANY DROPBOX ACCOUNT. THIS DROPBOX ACCOUNT HAS BEEN UTILISED TO RELEASE A VIRUS THROUGH ALL COMPANY FILES AS WELL AS UPLOAD A PORNOGRAPHIC IMAGE WITH PARTICULAR STAFF MEMBERS FACE 'PHOTOSHOPPED'. 'SUSPECT' HAS ALSO USED THE CEO'S COMPUTER NAME TO CREATE A FAKE LOG-IN ON DROPBOX TO ACCESS FILES / ACCOUNT LOG-INS / PASSWORDS. ALL LINKING TO AN IP ADDRESS THAN CAN BE TRACED NEAR SUSPECT WORKPLACE. ENTER THE DETAILS OF ANY AVAILABLE EVIDENCE OF THE INCIDENT: DROPBOX SHOWS ALL ACCOUNTS / EXTERNALS / APPS ETC THAT LOG-IN TO CERTAIN ACCOUNTS AND TWO IP ADDRESSES ALSO LINKED TO ACCESSING WORK COMPUTER ARE SHOWN HERE ON DROPBOX: IP Sch4p4(6) WAS DISCOVERED 17/6/15 AFTER FIRST REPORT WAS SUBMITTED AND REGISTERS TO BE NEAR SUSPECT WORKPLACE, AN EARLY IP ADDRESS ALREADY SUBMITTED IN REPORT HAS BEEN TRACED TO BE NEAR SUSPECT RESIDENCE IN SEMI-REMOTE AREA NEAR Sch4p4(6) IS THE VICTIM WILLING TO MAKE A FORMAL POLICE STATEMENT AND ATTEND COURT IN RELATION TO THE MATTER BEING REPORTED?: YES DID ANYONE ELSE WITNESS THE INCIDENT?: YES OFFENCE MODULE (ARN_B68G_UCY8) ---------- SELECT THE TYPE OF CYBERCRIME THAT BEST DESCRIBES THE INCIDENT YOU WOULD LIKE TO REPORT: ATTACKS ON A COMPUTER SYSTEM OR VIRUS CHOOSE THE BEST DESCRIPTION OF THE COMPUTER SYSTEM ATTACK: SOMEONE HAS ACCESSED A COMPUTER SYSTEM OR ONLINE ACCOUNT WITHOUT AUTHORISATION IN MORE DETAIL, DESCRIBE THE COMPUTER SYSTEM ATTACK: COMPANY DROPBOX HAS BEEN VIOLATED AND HAS BEEN FOUND TO HAVE BEEN LOGGED IN BY AN OUTSIDE SOURCE. A VIRUS HAS BEEN RELEASED DOING THOUSANDS OF DOLLARS WORTH OF DAMAGE TO COMPANY FILES AS WELL AS OTHER COMPANIES CONNECTED TO COMPANY DROPBOX. FOUR DUPLICATES OF A PORNOGRAPHIC IMAGE CONTAINING A 'PHOTOSHOPPED' IMAGE OF A STAFF MEMBER HAS BEEN 'HIDDEN' WITHIN THE COMPANY FILES FOR ALL TO ACCESS. THE IP ADDRESS ASSOCIATED WITH COMMON DATES CAN BE TRACED TO TWO SOURCES: Sch4p4(6)) Sch4p4(6) (Sch4p4(6)). (OTHER BREACHES ASSOCIATED WITH THESE IP ADDRESSES HAVE ALSO OC

Reports:

General report

Occurrence:	QP1500844884 Hacking / Misuse - Cyber [0761] @17/06/2015 21:55 (Sch4p4(6) (Patrol group: CITY CENTRAL, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, Stats are
Task:	T1502225878 [Init rpt - Closed] Due: 19/06/2015 19:07 #4028025 HICKS, S. ->#4028025 HICKS, S. [Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1500844884 Hacking / Misuse - Cyber [0761]

@17/06/2015 21:55 (Sch4p4(6)
Author: #4019576 LEBOYDRE, M.
Report time: 17/06/2015 21:55
Entered by: #4028025 HICKS, S.
Entered time: 18/06/2015 19:13
Remarks: Hacking / Misuse - Cyber [0761]. Sch4p4(6) Brisbane City. Victim: Sch4p4(6) Suspect: Sch4p4(6)

Narrative:
MO

Offence Module (ARN_6R4X_8YFF)

Select the type of cybercrime that best describes the incident you would like to report: Online identity theft
Identify one or more account types which have been compromised: Other: Company Shared Dropbox Account
Describe how it become apparent that the account(s) had been compromised: Virus was released through our Company Dropbox Account via a staff members account. IP Address is apparent to have logged in to Dropbox Account from an outside source Has there been any indication that the compromised account has been used by the scammer?: Yes
Based on the previous response, how has the account been used?: To embarrass or misrepresent the account owner, such as on social media
Has the bank or service provider been notified about the lost account information?: No

Method Module (ARN_6R4X_8YFF)

Choose one or more options of where the incident occurred: Work Computer
Enter the date when the incident occurred on, or the start date if the incident occurred over a period of time: 19/05/2015
Enter the end date if the incident occurred over a period of time: 17/06/2015
Is the incident still ongoing, or behaviour still happening?: Yes
In detail, describe the incident and each of the events that occurred and why you believe this is a criminal offence: Staff share a company Dropbox and one of the staff members targeted by 'suspect' noticed outside log-ins on their company Dropbox Account. This Dropbox account has been utilised to release a virus through all company files as well as upload a pornographic image with particular staff members face 'photoshopped'. 'Suspect' has also used the CEO's Computer Name to create a fake log-in on Dropbox to access files / account log-ins / passwords. All linking to an IP address than can be traced near suspect workplace.
Enter the details of any available evidence of the incident: Dropbox shows all accounts / externals / apps etc that log-in to certain accounts and two IP Addresses also linked to accessing work computer are shown here on Dropbox: Sch4p4(6) was discovered 17/6/15 after first report was submitted and registers to be near suspect workplace. An early IP address already submitted in report has been traced to be near suspect residence in semi-remote area near Sch4p4(6)
Is the victim willing to make a formal police statement and attend court in relation to the matter being reported?: Yes
Did anyone else witness the incident?: Yes

Offence Module (ARN_B68G_UCY8)

Select the type of cybercrime that best describes the incident you would like to report: Attacks on a computer system or virus
Choose the best description of the computer system attack: Someone has accessed a computer system or online account without authorisation
In more detail, describe the computer system attack: Company Dropbox has been violated and has been found to have been logged in by an outside source. A virus has been released doing thousands of dollars worth of damage to Company files as well as other Companies connected to

Company Dropbox. Four duplicates of a pornographic image containing a 'photoshopped' image of a staff member has been 'hidden' within the Company files for all to access. The IP address associated with common dates can be traced to two sources: Sch4p4(6) . (Other breaches associated with these IP addresses have also occurred including 'Identity Theft')
Provide details of the damage suffered from the attack: Company computers have been breached and accessed via 4 IP Addresses that appear to belong to one person alone. Over 80% of company files have been erased, corrupted and breached via the virus causing thousands of dollars worth of damage to private files as well as weeks of work to rebuild such files and links associated. Staff members have been emotionally affected by such pornographic exposure to the point where they feel they are no longer safe in the 'tech environment'. All computers and accounts contain passwords which are changed on a regular basis which means such a person has the knowledge and experience to 'hack' their way into secure accounts. Emails have been sent to Company Founder containing threatening material on a personal attack against a staff member using a name found on their Facebook account.

Method Module (ARN_B68G_UCY8)

Choose one or more options of where the incident occurred: Email: aol, Work Computer, Other: Company Dropbox
Enter the date when the incident occurred on, or the start date if the incident occurred over a period of time: 04/05/2015
Enter the end date if the incident occurred over a period of time: 16/06/2015
Is the incident still ongoing, or behaviour still happening?: Yes
In detail, describe the incident and each of the events that occurred and why you believe this is a criminal offence: 4.5.15: A virus was released using a staff members company Dropbox account that damaged thousands of dollars and work hours worth of company files as well as files of other companies also connect to company dropbox. 7.5.15: Emails were sent to company Founder in regards to staff in order to potentially have them fired using a name found on one of the staff members Facebook account. 12.6.15: 4 copies of a pornographic image with a staff members face 'photoshopped' on was placed within certain files within company dropbox using a staff members account. 15.6.15: 4 IP Addresses have been traced to breaching a work computer, accessing files, reading information and also found to have logged into a staff members Dropbox to upload the virus and pornographic image.
Enter the details of any available evidence of the incident: Dropbox shows the 2 IP Addresses of an outside source that has been linked to most breaches. Tech Manager set a 'trap' and traced the same 2 IP Addresses to be accessing the work computer as well as Dropbox account. The emails sent have been disregarded due to their 'false' appearance and obvious personal attack on innocent staff members.
Is the victim willing to make a formal police statement and attend court in relation to the matter being reported?: Yes
Did anyone else witness the incident?: Yes

GENERAL REPORT

IP Address Details (ARN_6R4X_8YFF)

Complainant IP Address: Sch4p4(
Date/Time: 17/06/2015 21:55:19
Confirmation IP Address: Not submitted
Date/Time: Not submitted

IP Address Details (ARN_B68G_UCY8)

Complainant IP Address: 10.9.2.30
Date/Time: 17/06/2015 14:36:34
Confirmation IP Address: Not submitted

Date/Time: Not submitted

Suspect Module (ARN_6R4X_8YFF)

SUSPECT 1

Suspect Type: Business
Given names: Sch4p4
Surname: Sch4p4(6
Business name: Sch4p4(6)
Country: Australia
State: QLD
Suburb: Sch4p4(6)
Postcode: Sch
Phone number: Sch4p4(6)
Email address: Sch4p4(6)
IP address: Sch4p4(6)
Describe how you got the IP address and why is it linked to the suspect?: IP Address was discovered to have logged-in on our company Dropbox account under a staff members account. This account has been hacked to release a virus through all company files as well as post 4 copies of the same pornographic image through company files for all staff to view.
Other additional information about the suspect: Suspect is an IT Expert who's job (with Sch4p4 Sch4p4(6) Sch4p4(is to access many Brisbane-Based companies secure files to resolve internal and external issues. Suspect has been known to use this knowledge to tarnish other companies files in the past and 'brag' about his knowledge of other companies account / password /access details. This person is Sch4p4(6)) and has had access to two of current computers, one in which he has used to release virus and upload pornographic image.

Suspect Module (ARN_B68G_UCY8)

SUSPECT 1

Suspect Type: I don't know
Country: Australia
State: QLD
Suburb: BRISBANE CITY
Postcode: 4000
IP address: 110.175.177.252
Describe how you got the IP address and why is it linked to the suspect?: We found the following IP Addressed that have logged in to our Dropbox Account that do not belong to anyone in our Company: Sch4p4(6) Our web/tech developer set up a 'trap' which the 'hacker' clicked on and it was the same IP addresses as above as well as: Sch4p4(6)
Other additional information about the suspect: The only person outside of our company that has had access to two of our laptops is an Sch4p4(6)
Works from his office in Sch4p4(Also is the IT expert for other companies around Brisbane area. We do not wish to point fingers however certain information seems to match up with his expertise. He is know to Sch4p4(6) a previous workplace.

Details

Queensland Police Service

Report no.:	QP1501091218
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	12/06/2015 12:00 -
Reported time:	12/06/2015 12:00
Place of offence:	SUBURB - BRISBANE CITY, BRISBANE CITY, QLD Australia 4000 (Patrol group: CITY CENTRAL, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, Stats area: 305011143) (Cannot be merged - merge limit reached)
Clearance status:	Finalised
Summary:	Hacking / Misuse - Cyber [0761]; Address: SUBURB - BRISBANE CITY; Victim: Sch4p4(6) ; Offender: Sch4p4(6) : Sch4p4(6
Concluded summary:	

Printed: 06/08/2017 21:08 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Patrol group: BAYSIDE, Court Dist./Div.: BRISBANE/WYNNUM, Region: BRISBANE, District: SOUTH BRISBANE, Division: WYNNUM, Stats area: 305111364) (GNAF - no longer curre] / [Crime: Solved]
   Offender: [Sch4p4(6) Patrol group: INNER WEST, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: INDOOROOPILLY, Stats area: 305071318, NHW: INDOOROOPILLY] / Status: [Notice to appear (1b)]
   Cleared Unit: [BRISBANE CITY CIB (POLICE - CITY POLICE STATION, , BRISBANE CITY, QLD Australia 4000 (Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, Stats area: 305011143))] / [03/08/2015]

Modus operandi:

1. Location: Public place. Victim age: Male adult (over 18). Relationship to offender: Not known. Other behavior at scene: Unknown. Method of escape: Unknown. No. of offenders/suspects: One. Free text keywords: ON THE NOMINATED DATE, THE OFFENDER HAS GAINED ACCESS TO THE VICTIM'S FACEBOOK ACCOUNT AND OBTAINED THE 10 APPROVAL CODES REQUIRED TO GAIN FURTHER ACCESS IF THE PASSWORDS ARE CHANGED. THE OFFENDER HAS ALSO, AT THE REQUEST OF OTHERS, ALTERED THE DETAILS ON THE ACCOUNT BY UNBLOCKING AN UNKNOWN NUMBER OF PEOPLE. THIS INFORMATION WAS THEN PROVIDED TO A THIRD PARTY WITHOUT THE KNOWLEDGE OF THE VICTIM..

Reports:

General report

Occurrence:	QP1501091218 Hacking / Misuse - Cyber [0761] @12/06/2015 12:00 (SUBURB - BRISBANE CITY, BRISBANE CITY, QLD Australia 4000 (Patrol group: CITY CENTRAL, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY,
Task:	T1502880068 [Init rpt - Closed] Due: 07/08/2015 12:57

#4033330 HAMREY, K. ->#4033330 HAMREY, K. [Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1501091218 Hacking / Misuse - Cyber [0761] @12/06/2015 12:00 (SUBURB - BRISBANE CIT

Author: #4020818 FLEMING, J.
Report time: 12/06/2015 12:00
Entered by: #4033330 HAMREY, K.
Entered time: 06/08/2015 12:59
Remarks: Hacking / Misuse - Cyber [0761]; Address: SUBURB - BRISBANE CITY; Sch4p4(6) ; Offender: Sch4p4(6) 4

Narrative:

MO

On the nominated date, the offender has gained access to the victim's Facebook account and obtained the 10 approval codes required to gain further access if the passwords are changed. The offender has also, at the request of others, altered the details on the account by unblocking an unknown number of people. This information was then provided to a third party without the knowledge of the victim.

GENERAL REPORT

Offence as per MO. This offence was identified by Police during Operation MIKE CROMWELL. On the 03/08/2015, detectives attended the Brisbane City Watch House and conducted an ROI with the offender. Offender declined to make any comment in relation to this offence. Based on other evidence obtained, the offender was issued with a NTA in relation to this and other matters. SOC not required. Nil CCTV. Insurance not applicable. Nil witnesses

Details

Queensland Police Service

Report no.:	QP1501359754
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	20/09/2015 00:00 - 20/09/2015 23:59
Reported time:	21/09/2015 13:54
Place of offence:	Sch4p ROAD VILLAGE, Sch4p4(6) (Patrol group: EAST GATEWAY, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: HENDRA, Stats area: 305071604)
Clearance status:	Finalised
Operation name:	ACORN 1
ACORN #:	ARNA3H6E6UE
Summary:	Hacking / Misuse - Cyber. Address: Sch4p4(6) . Victim: GHOBRIAL, Sch4p4(6)
Concluded summary:	

Printed: 06/08/2017 21:21 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) Patrol group: RIVERSIDE, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: SOUTH BRISBANE, Division: MORNINGSIDE, Stats area: 305091258) (E-mail) Sch4p4(6)] / [Crime: Solved]
   Offender: [Sch4p4(6)), Id #:11238612 DL:QLD:Sch4p4(6) / Status: [Notice to appear (1b)]
   Cleared Unit: [CALOUNDRA CIB (1 GREGSON PL, CALOUNDRA, QLD Australia 4551 (Patrol group: SUNSHINE COAST SOUTHERN, Court Dist./Div.: MAROOCHYDORE, Region: CENTRAL, District: SUNSHINE COAST, Division: CALOUNDRA, Stats area: 309056721))] / [06/12/2016]

Modus operandi:

1. Location: Medical. Subtype: Dental surgery. Location specific: Unknown. Occupancy: Not known. Security measures: Unknown. Victim age: Male adult (over 18). Victim's prior actions: Unknown. Victim injuries sustained: No injury. Relationship to offender: Not known. Other behavior at scene: Unknown. Method of escape: Unknown. No. of offenders/suspects: Unknown. Computer hacking method: Access/interfere data. Communication device: No device/unknown. Free text keywords: *CALL RECEIVED FROM INFORMANT/VICTIM Sch4p4(6) L VIA INTAKE FACILITY AT FRAUD & CYBER CRIME GROUP. CALL TAKEN BY DS MILLARD AND REFERRED TO CICIU DUE TO COMPUTER HACKING OFFENCE. DSC HALLETT CONTACTED INFORMANT WHO PROVIDED THAT HE WAS THE OWNER OF BUSINESS Sch4p4(6) QLD. Sch4p4(6 STATED THAT HE HAD PURCHASED THIS BUSINESS SOME TIME AGO AND WAS CURRENTLY GOING THROUGH AN ONGOING CIVIL DISPUTE OVER THE BUSINESS WITH THE PREVIOUS OWNERS. Sch4p4(6 STATED THAT HE HAD BECOME AWARE OF CERTAIN FILES RELATING TO THESE LEGAL PROCEEDINGS BEING DELETED FROM THE COMPANY'S DROP-BOX ACCOUNT AND COMPANY EMAIL ACCOUNT. Sch4p4(6 STATED THAT HE HAD NOW TAKEN STEPS AND CHANGED ALL PASSWORDS TO THE ACCOUNTS, HOWEVER BELIEVES THAT THE PREVIOUS OWNERS OF THE COMPANY ARE THE ONES RESPONSIBLE FOR HACKING INTO THE BUSINESSES IT SYSTEM. Sch4p4(6 BELIEVES THIS HAS OCCURRED DUE TO Sch MISTAKENLY SENDING THE PREVIOUS OWNERS AND EMAIL APPROXIMATELY TWO YEARS AGO WHICH CONTAINED THE NEW PASSWORD TO THE Sch ACCOUNT WHICH Sch4p4(6 NOW REALISE HE CONTINUED TO USE FOR THE BUSINESS. Sch4p4(6 WAS PROVIDED ADVICE AS FAR AS PASSWORD PROTECTION AND USING A BUSINESS

DROP-BOX ACCOUNT RATHER THAN A PERSONAL ONE TO PROTECT FILES. Sch4p4(6 STATED THAT HE HAS BACK-UPS OF ALL DELETED DOCUMENTS, HOWEVER WISHES TO PROCEED WITH CRIMINAL PROCEEDING AGAINST THE PERSONS RESPONSIBLE FOR THIS HACK. DUE TO THE BUSINESS BEING LOCATED IN THE WAVELL HEIGHTS AREA, THIS COMPLAINT WILL BE REFERRED TO POLICELINK FOR A CREATION OF A QP AND FORWARDING TO THE RELEVANT NORTH BRISBANE DISTRICT CIB FOR INVESTIGATION. Sch4p4(6 HAS BEEN ADVISED THAT ONCE THIS MATTER HAS BEEN REFERRED TO THE INVESTIGATING JURISDICTION HE IS BEST TO LIAISE WITH THE ASSIGNED INVESTIGATING OFFICER IN RELATION TO A FULL DOWNLOAD OF THE BUSINESS SERVER ETC IN REGARD TO SECURING EVIDENCE OF THIS OFFENCE. OFFENCE MODULE SELECT THE TYPE OF CYBERCRIME THAT BEST DESCRIBES THE INCIDENT YOU WOULD LIKE TO REPORT ONLINE IDENTITY THEFT IDENTIFY ONE OR MORE ACCOUNT TYPES WHICH HAVE BEEN COMPROMISED EMAIL, OTHER: DROP BOX DESCRIBE HOW IT BECOME APPARENT THAT THE ACCOUNT(S) HAD BEEN COMPROMISED CONTENT HAS BEEN DELETED WITH OUT ME DOING IT. HAS THERE BEEN ANY INDICATION THAT THE COMPROMISED ACCOUNT HAS BEEN USED BY THE SCAMMER? YES BASED ON THE PREVIOUS RESPONSE, HOW HAS THE ACCOUNT BEEN USED? OTHER: TO DELETE EVIDENCE HAS THE BANK OR SERVICE PROVIDER BEEN NOTIFIED ABOUT THE LOST ACCOUNT INFORMATION? NO VICTIM MODULE WHY ARE YOU REPORTING THIS INCIDENT? I AM THE VICTIM HAS THIS INCIDENT BEEN PREVIOUSLY REPORTED TO THE ACORN, AND IS THE ACORN REFERENCE NUMBER AVAILABLE? NO HAS ANY OTHER PERSON, WEBSITE OR AGENCY BEEN INFORMED OF THE INCIDENT? YES BASED ON THE PREVIOUS RESPONSE, CHOOSE WHO THE INCIDENT HAS BEEN REPORTED TO OTHER: OUR IT COMPANY GIVEN NAMES Sch4p4(6 SURNAME Sch4p4(6) DATE OF BIRTH Sch4p4(6 4 COUNTRY AUSTRALIA STATE QLD SUBURB ROCHEDALE SOUTH POSTCODE 4123 STREET ADDRESS Sch4p4(6) OTHER ADDITIONAL INFORMATION ABOUT THE VICTIM I AM A BUSINESS OWNER. THERE HAVE BEEN ISSUES WITH THE PREVIOUS OWNERS AND I AM CONCERNED THEY ARE DELETING EVIDENCE. I HAVE AN IP NUMBER WHICH I KNOW MY DROPBOX WAS ACCESSED FROM. SUSPECT MODULE (NO ANSWERS) METHOD MODULE CHOOSE ONE OR MORE OPTIONS OF WHERE THE INCIDENT OCCURRED

Reports:

General report

Occurrence:	QP1501359754 Hacking / Misuse - Cyber [0761] @21/09/2015 13:54 (Sch4p4(6) VILLAGE, Sch4p4(6) (Patrol group: EAST GATEWAY, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Divisi
Task:	T1503565095 [Init rpt - Closed] Due: 24/09/2015 14:52 #4028726 SCOTT, B. ->#4028726 SCOTT, B. [Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1501359754 Hacking / Misuse - Cyber [0761] @21/09/2015 13:54 (Sch4p4(6)
Author:	#4021148 HALLETT, H.
Report time:	21/09/2015 13:54
Entered by:	#4028726 SCOTT, B.
Entered time:	23/09/2015 15:07
Remarks:	Hacking / Misuse - Cyber. Sch4p4(6) . Victim: Sch4p4(6)

Narrative:
MO

**Call received from informant/victim Sch4p4(6) via intake facility at Fraud & Cyber Crime Group. Call taken by DS MILLARD and referred to CICIU due to computer hacking offence. DSC HALLETT contacted informant who provided that he was the owner of business Sch4p4(6) QLD. Sch4p4(stated that he had purchased this business some time ago and was currently going through an ongoing civil dispute over the business with the previous owners. Sch4p4(stated that he had become aware of certain files relating to these legal proceedings being deleted from the company's drop-box account and*

company email account. Sch4p4(*stated that he had now taken steps and changed all passwords to the accounts, however believes that the previous owners of the company are the ones responsible for hacking into the businesses IT system.* Sch4p4(*believes this has occurred due to* Sc *mistakenly sending the previous owners and email approximately two years ago which contained the new password to the* Sc *account which* Sch4p4(*now realise he continued to use for the business.* Sch4p4(*was provided advice as far as password protection and using a business drop-box account rather than a personal one to protect files.* Sch4p4(*stated that he has back-ups of all deleted documents, however wishes to proceed with criminal proceeding against the persons responsible for this hack. Due to the business being located in the Wavell Heights area, this complaint will be referred to policelink for a creation of a QP and forwarding to the relevant North Brisbane District CIB for investigation.* Sch4p4(*has been advised that once this matter has been referred to the investigating jurisdiction he is best to liaise with the assigned investigating officer in relation to a full download of the business server etc in regard to securing evidence of this offence.*

Offence Module

Select the type of cybercrime that best describes the incident you would like to report

Online identity theft

Identify one or more account types which have been compromised

Email, Other: Drop Box

Describe how it become apparent that the account(s) had been compromised

Content has been deleted with out me doing it.

Has there been any indication that the compromised account has been used by the scammer?

Yes

Based on the previous response, how has the account been used?

Other: To delete evidence

Has the bank or service provider been notified about the lost account information?

No

Victim Module

Why are you reporting this incident?

I am the victim

Has this incident been previously reported to the ACORN, and is the ACORN reference number available?

No

Has any other person, website or agency been informed of the incident?

Yes

Based on the previous response, choose who the incident has been reported to

Other: Our IT Company

Given names

Sch4p

Surname

Sch4p

Date of birth

Sch4p4 4

Country

Australia

State

QLD

Suburb

ROCHEDALE SOUTH

Postcode

4123

Street address

Sch4p4(6)

Phone number

Sch4p4(6

Email address

Sch4p4(6)

Other additional information about the victim

I am a business owner. there have been issues with the previous owners and I am concerned they are deleting evidence. I have an IP number which I know my Dropbox was accessed from.

Suspect Module (no answers)

Method Module

Choose one or more options of where the incident occurred

Email: comapny email, Other: Drop Box

Enter the date when the incident occurred on, or the start date if the incident occurred over a period of time

S /09/2015

Enter the end date if the incident occurred over a period of time

S /09/2015

Is the incident still ongoing, or behaviour still happening?

Yes

In detail, describe the incident and each of the events that occurred and why you believe this is a criminal offence

I am not sure when it started however we did notice files being deleted from both my email and Drop box. These files relate to a potential law suit with a previous employee.

Enter the details of any available evidence of the incident

I have the IP address used to access my dropbox. The IP number is Sch4p4(6)

Is the victim willing to make a formal police statement and attend court in relation to the matter being reported?

Yes

Did anyone else witness the incident?

Yes

Loss Module

Did the incident involve a loss of money, personal information, goods or data?

Yes

Choose an option which best describes the type of loss

Other: Confidential Business information

Describe the other type of loss that occurred

As stated loss of evidence against a former employee.

Enter the estimated value of the loss (in Australian Dollars)

0

GENERAL REPORT

This is an ACORN referred occurrence relating to an alleged cybercrime however the victim has not provided sufficient details to identify either the suspect or the offence location. . [Commissioner Circular 19/2014 incorporating OPM 2.5.12 and 2.6.8 refers].

Please have enquiries conducted with the victim in this matter with a view to establishing the identity of the suspect, offence location and any other information to assist in an investigation.

Please refer to the attached external document for full details of the ACORN referral.

If it is established that the offence location is in another jurisdiction (not Queensland) please ensure all details of enquiries made are recorded on the enquiry log on this occurrence and then forward a task via QPRIME procedures to org unit 3343 (ACORN manager) for attention.

Details

Queensland Police Service

Report no.:	QP1600062084
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	18/12/2015 00:00 - 18/12/2015 23:59
Reported time:	11/01/2016 08:54
Place of offence:	Sch4p4(6) (Patrol group: TOWNSVILLE, Court Dist./Div.: TOWNSVILLE, Region: NORTHERN, District: TOWNSVILLE, Division: TOWNSVILLE, Stats area: 345057041, Beat: TOWNSVILLE COMMUNITY)
Clearance status:	Finalised
Operation name:	ACORN1
ACORN #:	ARNYKDP763B
Summary:	Hacking / Misuse - Cyber. 22/1-7 Gregory Street, North Ward. Victim: Sch4p4(Suspect: Sch4p4(6) DOB: Sch4p4(6
Concluded summary:	

Printed: 06/08/2017 20:51 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Patrol group: TOWNSVILLE, Court Dist./Div.: TOWNSVILLE, Region: NORTHERN, District: TOWNSVILLE, Division: TOWNSVILLE, Stats area: 345057041, Beat: TOWNSVILLE COMMUN] / [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: RIVERSIDE, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: SOUTH BRISBANE, Division: MORNINGSIDE, Stats area: 305091397) (30 OLIVE ST, MORNI] / Status: [Notice to appear (1b)]
   Cleared Unit: [TOWNSVILLE CIB (8-32 STANLEY ST, TOWNSVILLE CITY, QLD Australia 4810 (Patrol group: TOWNSVILLE, Court Dist./Div.: TOWNSVILLE, Region: NORTHERN, District: TOWNSVILLE, Division: TOWNSVILLE, Stats area: 345057003))] / [25/01/2016]

Modus operandi:

1. Location: Dwelling. Subtype: Flat. Location specific: Unknown. Building: Unit block. Occupancy: Occupied. Subtype: Single. Security measures: Unknown. Victim age: Female adult (over 18). Victim's prior actions: At home. Victim injuries sustained: No injury. Relationship to offender: Not known. Other behavior at scene: Telephone used - mobile. Method of escape: Unknown. No. of offenders/suspects: One. Free text keywords: VICTIM STATES THAT THE SUSPECT GAINED ACCESS TO THEIR MOBILE PHONE AND TOOK DATA FROM THAT DEVICE, THEY ARE NOW USING THIS DEVICE AGAINST THE VICTIM .

Reports:

General report

Occurrence:	QP1600062084 Hacking / Misuse - Cyber [0761] @11/01/2016 08:54 Sch4p4(6) (Patrol group: TOWNSVILLE, Court Dist./Div.: TOWNSVILLE, Region: NORTHERN, District: TOWNSVILLE, Division: TOWNSVILLE, Stats area: 3450
Task:	T1600139672 [Init rpt - Closed] Due: 12/01/2016 10:28 #4029292 GILCHRIST, C. ->#4029292 GILCHRIST, C.

[Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1600062084 Hacking / Misuse - Cyber [0761] @11/01/2016 08:54 (Sch4p4(6)

Author: #4020292 COX, D.
Report time: 11/01/2016 08:54
Entered by: #4029292 GILCHRIST, C.
Entered time: 11/01/2016 10:28
Remarks: Hacking / Misuse - Cyber. Sch4p4(6) Victim: MULLER, Sch4p4(6) . Suspect: Sch4p4 Sch4p4(6)

Narrative:

MO

Victim states that the suspect gained access to their mobile phone and took data from that device, they are now using this device against the victim

GENERAL REPORT

This is an ACORN referred report relating to an alleged cybercrime and which appears to have been committed in Queensland.

Please refer to the attached external documents for full details of the ACORN referral and instructions concerning investigation obligations.

Investigators of cybercrime related matters should be aware of OPM 1.11 (Cybercrime reporting), 2.5.12 (Investigating cybercrime) and 2.6.8 (Specialist electronic and cybercrime investigations).

If investigations establish an offence location and it is in another jurisdiction (not Queensland) please ensure that all details of enquiries are recorded in the occurrence enquiry log. Change occurrence location to reflect the offence location and cancel the occurrence. Send a task to org unit 3343 (ACORN manager) for attention and referral of ACORN report to the responsible agency.

NOTE: There is no ACORN investigation unit within Fraud and Cyber Crime Group. Advice concerning investigating cybercrime can be obtained from the Cyber and Identity Crime Investigation Unit by internal email – SCC Cyber & ID Crime Investigation Unit

Victim states they are now working in Sch4p4 however email contact is possible to establish the events of the QLD offence. SOC not required.

Details

Queensland Police Service

Report no.: QP1600567114
Occurrence Type: Hacking / Misuse - Cyber [0761]
Occurrence time: 17/03/2016 00:00 - 17/03/2016 23:59
Reported time: 01/04/2016 10:44
Place of offence: Sch4p4(6) (Patrol group: GLADSTONE, Court Dist./Div.: GLADSTONE, Region: CENTRAL, District: CAPRICORNIA, Division: GLADSTONE, Stats area: 330103366)
Clearance status: Finalised
Operation name: Intranet Occurrences
Summary: Occurrence Type: Stealing by conversion or by a trick (0840); Occurrence Address: Sch4p4(6); Victim 1: Sch4p4(6); Suspect 1: Sch4p4(6); ***ADDENDUM 05.08.2016 - offences of Fraud Imposition and Hacking/Misuse - Cyber added for offender Sch4p4(6)
Concluded summary:

Printed: 07/08/2017 09:32 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Patrol group: GLADSTONE, Court Dist./Div.: GLADSTONE, Region: CENTRAL, District: CAPRICORNIA, Division: GLADSTONE, Stats area: 330103366) (Land line) Sch4p4(6))] / [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: GLADSTONE, Court Dist./Div.: GLADSTONE, Region: CENTRAL, District: CAPRICORNIA, Division: GLADSTONE, Stats area: 330103366) (Mobile telephone) Sch4p4(6)] / Status: [Notice to appear (1b)]
   Cleared Unit: [GLADSTONE CIB (12-14 YARROON ST, GLADSTONE CITY, QLD Australia 4680 (Court Dist./Div.: GLADSTONE, Region: CENTRAL, District: CAPRICORNIA, Division: GLADSTONE, Stats area: 330103366) (Land line) 0749713244)] / [05/08/2016]
2. [0755/ Fraud, Imposition (Other)] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Patrol group: GLADSTONE, Court Dist./Div.: GLADSTONE, Region: CENTRAL, District: CAPRICORNIA, Division: GLADSTONE, Stats area: 330103366) (Land line) Sch4p4(6))] / [Crime: Solved]
   Offender: [Sch4p4(6) Id #:Sch4p4(6) :405010127 DL:QLD:Sch4p4(6) / Status: [Notice to appear (1b)]
   Cleared Unit: [GLADSTONE CIB (12-14 YARROON ST, GLADSTONE CITY, QLD Australia 4680 (Court Dist./Div.: GLADSTONE, Region: CENTRAL, District: CAPRICORNIA, Division: GLADSTONE, Stats area: 330103366) (Land line) 0749713244)] / [05/08/2016]
3. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Patrol group: GLADSTONE, Court Dist./Div.: GLADSTONE, Region: CENTRAL, District: CAPRICORNIA, Division: GLADSTONE, Stats area: 330103366) (Land line) Sch4p4(6))] / [Crime: Solved]
   Offender: [Sch4p4(6) , Sch4p4(6) DL:QLD:Sch4p4(6) / Status: [Notice to appear (1b)]
   Cleared Unit: [GLADSTONE CIB (12-14 YARROON ST, GLADSTONE CITY, QLD Australia 4680 (Court Dist./Div.: GLADSTONE, Region: CENTRAL, District: CAPRICORNIA, Division: GLADSTONE, Stats area: 330103366) (Land line) 0749713244)] / [05/08/2016]

Modus operandi:

1. Location: Commercial. Subtype: Bank. Other behavior at scene: Unknown. No. of offenders/suspects: One. Free text keywords: ON THE 17TH OF MARCH 2016 THE SUSPECT AMBROSE HAS A ACCESSED THE VICTIMS, Sch4p4(6) Sch4p4(6) BANK ACCOUNTS AND TRASNFERED A SUM OF MONEY TO THE VALUE OF $2482.00 TO Sch OWN ACCOUNTS WITHOUT PERMISSION FROM THE VICTIM..

Reports:

General report

Occurrence:	QP1600567114 Hacking / Misuse - Cyber [0761] @01/04/2016 10:44 (Sch4p4(6) (Patrol group: GLADSTONE, Court Dist./Div.: GLADSTONE, Region: CENTRAL, District: CAPRICORNIA, Division: GLADSTONE, Stats area: 330103366))
Task:	T1601360994 [Init rpt - Closed] Due: 02/04/2016 11:14 #4032652 ANQUETIL, S. ->#4032652 ANQUETIL, S. [Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1600567114 Hacking / Misuse - Cyber [0761] @01/04/2016 10:44 (Sch4p4(6)
Author:	#4032652 ANQUETIL, S.
Report time:	01/04/2016 10:44
Entered by:	#4032652 ANQUETIL, S.
Entered time:	01/04/2016 11:14
Remarks:	Occurrence Type: Stealing by conversion or by a trick (0840); Occurrence Address: Sch4p4(6) ; Victim 1: Sch4p4(6) Suspect 1: Sch4p4(6)

Narrative:

MO

On the 17th of March 2016 the suspect Ambrose has a accessed the victims,Sch4p4(6) , bank accounts and trasnfered a sum of money to the value of $2482.00 to Sc own accounts without permission from the victim.

GENERAL REPORT

The offence occured as per the MO. The victim Sch4p4(6) attended rockhampton police station to report a stealing offence. Sch4p4(6) Sc Sch4p4(6) and has been informaed that the money in bank accounts have been transfered to Sch4p4(6) . Sch4p4(6) stated that Sch4p4(6 may have had his wallet which may have contained his banking details. Sch4p4(6) banks with CUA and has provided Police with Emails of receipts, numbers and transactions listings. The transaction appears to have been done through online banking and it is unlikely CCTV footage is avaliabe. Sch4p4(6) did not provide statement at time of report however advised that one will be required. Documents to be scanned into occured and occurance to be detailed to Gladstone for investigation. . SOC not required.

Details

Queensland Police Service

Report no.:	QP1600907955
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	20/04/2016 00:01 - 20/04/2016 23:59
Reported time:	17/05/2016 15:40
Place of offence:	Sch4p4(6) (Patrol group: CITY CENTRAL, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, Stats area: 305011378, Beat: MILTON)
Clearance status:	Finalised
Operation name:	ACORN1
ACORN #:	ARNUAUERXH4
ACORN #:	ARNXFTTX38R
ACORN #:	ARNY4EPHRAX
Summary:	Hacking / Misuse - Cyber [0761]; Address: Sch4p4(6) Informant: Sch4p4(6) ; Victim: Sch4p4(6) Named Person: Sch4p4(6)
Concluded summary:	

Printed: 06/08/2017 21:19 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [7]
   Victim: [Sch4p4(6) (Patrol group: CITY CENTRAL, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISB] / [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: MOUNT GRAVATT, Court Dist./Div.: BRISBANE/HOLLAND PARK, Region: BRISBANE, District: SOUTH BRISBANE, Division: UPPER MOUNT GRAVATT, Stats area: 30511115] / Status: [Arrested (1a)]
   Cleared Unit: [BRISBANE CITY CIB (POLICE - CITY POLICE STATION, , BRISBANE CITY, QLD Australia 4000 (Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, Stats area: 305011143))] / [20/07/2016]

Modus operandi:

1. Location: Commercial. Other behavior at scene: Unknown. Method of escape: Unknown. No. of offenders/suspects: Unknown. Free text keywords: THE INFORMANT BELIEVES THAT THE NAMED PERSON HAS GAINED ACCESS TO THE COMPANY EMAILS AND TRANSFERRED MONEY INTO UNKNOWN ACCOUNTS. THE NAMED PERSON DID NOT HAVE PERMISSION TO DO THIS. .

Reports:

General report

Occurrence:	QP1600907955 Hacking / Misuse - Cyber [0761] @17/05/2016 15:40 (Sch4p4(6) (Patrol group: CITY CENTRAL, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, S
Task:	T1602125738 [Init rpt - Closed] Due: 24/05/2016 15:46

#4033330 HAMREY, K. ->#4033330 HAMREY, K. [Low]
QPS Investigative Task Workflow Initial Report Task and
Start Point QP1600907955 Hacking / Misuse - Cyber [0761]
@17/05/2016 15:40 (Sch4p4(6)

Author: #4011146 REYNOLDS, T.
Report time: 17/05/2016 15:40
Entered by: #4033330 HAMREY, K.
Entered time: 23/05/2016 16:07
Remarks: Hacking / Misuse - Cyber [0761]; Address: Sch4p4(6) ; Informant: Sch4p4(6) ; Victim: Sch4p4(6) ; Named Person: Sch4p4(6)

Narrative:
MO

The informant believes that the named person has gained access to the company emails and transferred money into unknown accounts.

The named person did not have permission to do this.

GENERAL REPORT

The informant states they have log files.

The informant has lodged three separate ACORN relating to this matter.

This is an ACORN referred report relating to an alleged cybercrime however the victim has not provided sufficient details to identify either the suspect or the offence location. Please refer to the attached external document for full details of the ACORN referral

Please conduct inquiries as per OPM 2.5.12 – Investigating cybercrime.

If it is established that the offence location is in another jurisdiction (not Queensland) please ensure all details of enquiries made are recorded on the occurrence enquiry log on this occurrence and then tasked to org unit 3343 (ACORN manager) for information.

Details

Queensland Police Service

Report no.: QP1601344681
Occurrence Type: Hacking / Misuse - Cyber [0761]
Occurrence time: 13/07/2016 23:59 - 19/07/2016 00:01
Reported time: 19/07/2016 15:24
Place of offence: Sch4p4(6) (Patrol group: INNER WEST, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: INDOOROOPILLY, Stats area: 305071084, NHW: INDOOROOPILLY 13)
Clearance status: Finalised
Summary: Hacking / Misuse - Cyber [0761] Occurrence Address: Sch4p4(6) Victim: Sch4p4(6) Business: Sch4p4(6) : Sch4p4(6)
Concluded summary:

Printed: 07/08/2017 09:30 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Patrol group: INNER WEST, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: THE GAP, Stats area: 305031048) (E-mail) Sch4p / [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: INNER WEST, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: INDOOROOPILLY, Stats area: 305071084, NHW: INDOOR] / Status: [Arrested (1a)]
   Cleared Unit: [FERNY GROVE PROPERTY CRIME TEAM] / [19/07/2016]

Modus operandi:

1. Location: Dwelling. Subtype: House. Occupancy: Occupied. Subtype: Multi. Victim features: Victimised at work. Victim age: Male adult (over 18). Victim's prior actions: At home. Victim injuries sustained: No injury. Relationship to offender: Employee. Behavior toward victim: Confidence. Victim resistance: None. Offender's reaction to resistance: Ignores. Other behavior at scene: Other. Method of escape: Unknown. No. of offenders/suspects: One. Computer hacking method: Access/interfere computer systems; Access/interfere data; Access/interfere programs. Communication device: Email. Free text keywords: BETWEEN TIMES AND DATE STATED THE OFFENDER HAS REMOVED THE COMPLAINANT PERMISSION TO ACCESS THE COMPANY WEBSITE, EMAIL ACCOUNT AND BANK ACCOUNTS. .

Reports:

General report

Occurrence: QP1601344681 Hacking / Misuse - Cyber [0761] @19/07/2016 15:24 Sch4p4(6) Sch4p4(6) (Patrol group: INNER WEST, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: INDOOROOPILLY, Stats ar
Task: T1602980436 [Init rpt - Closed] Due: 20/07/2016 15:24 #4034458 GLOGER, V. ->#4034458 GLOGER, V. [Low] QPS Investigative Task Workflow Initial Report Task and

Start Point QP1601344681 Hacking / Misuse - Cyber [0761] @19/07/2016 15:24 (Sch4p4(6)

Author: #4010861 SMITH, C.
Report time: 19/07/2016 15:24
Entered by: #4034458 GLOGER, V.
Entered time: 19/07/2016 15:34
Remarks: Hacking / Misuse - Cyber [0761] Occurrence Address: S Victim: Sch4p4(6) Business: Sch4p4(6) Offender: Sch4p4(6)

Narrative:

MO

Between times and date stated the offender has removed the complainant permission to access the company website, email account and bank accounts.

GENENERAL REPORT

Offence occurred as per MO. SOC not required. No CCTV Footage. Not CMG related.

This matter is a part of another ongoing investigation relating to the offender as conducting numerous fraudulent transactions from the company's bank account.

Details

Queensland Police Service

Report no.:	QP1601366042
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	21/01/2016 09:00 - 28/06/2016 16:30
Reported time:	22/07/2016 14:32
Place of offence:	Sch4p4(6) (Patrol group: GYMPIE, Court Dist./Div.: GYMPIE, Region: CENTRAL, District: WIDE BAY BURNETT, Division: GYMPIE, Stats area: 315103624)
Clearance status:	Finalised
Operation name:	Intranet Occurrences
Summary:	Occurrence Type: Stealing from other specified buildings (including ATM transactions) (0835); Occurrence Address: Sch4p4(6) Victim 1: Sch4p4(Sch4 Suspect 1: Sch4p4(6) Offence type corrected to Fraud embezzlement
Concluded summary:	

Printed: 07/08/2017 10:11 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [23]
   Victim: [Sch4p4(6) (Patrol group: BUNDABERG, Court Dist./Div.: BUNDABERG, Region: CENTRAL, District: WIDE BAY BURNETT, Division: BUNDABERG, Stats area: 315051822, Beat: BUNDABERG] / [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: GYMPIE, Court Dist./Div.: GYMPIE, Region: CENTRAL, District: WIDE BAY BURNETT, Division: GYMPIE, Stats area: 315103624)), Id #:Sch4p4(6) :Sch4p4(6) DL:QL] / Status: [Arrested (1a)]
   Cleared Unit: [GYMPIE STATION (40 CHANNON ST, GYMPIE, QLD Australia 4570 (Patrol group: GYMPIE, Court Dist./Div.: GYMPIE, Region: CENTRAL, District: WIDE BAY BURNETT, Division: GYMPIE, Stats area: 315103624) (Land line) 0754801033)] / [08/08/2016]

Modus operandi:

1. Location: Commercial. Subtype: Bank. Other behavior at scene: Unknown. No. of offenders/suspects: One. Free text keywords: THE COMPLAINANT IS THE GENERL MANAGER OF Sch4p4(6) , WHICH OPERATES 24 BRANCHES ACROSS QUEENSLAND. THE GENERAL MANAGER IS BASED IN Sch4p4(6) BUT RESIDES IN Sch4p4(Sch THE NOMINATED SUSPECT, AN EMPLOYEE OF Sch4p4(6) Sch4p RESIDES IN Sch4p4(AND WAS EMPLOYED AS BANK OFFICER AT THE Sch4p4(BRANCH. BETWEEN JANUARY AND JULY 2016, THE SUSPECT IN HIS CAPACITY AS A Sch4 Sch4p4(6 HAS CREATED A BOGUS ACCOUNT IN HIS MOTHER'S NAME THEN CREATED AN ELECTRONIC TRANSFER OF FUNDS FROM AN ACCOUNT HELD BY Sc Sch4p4(Sch4p4(6) VARIOUS AMOUNTS OF MONEY DURING THIS PERIOD WERE TRANSFERED TO THIS BOGUS ACCOUNT ALSO WITH Sch4p4(6) Sch4 THEN TRANSFERED THIS MONEY TO AN ACCOUNT IN HIS NAME. THE COMPLAINANT CAN EVIDENCE THE ELECTRONIC TRANSFER OF MONIES..

Reports:

General report

Occurrence:	QP1601366042 Hacking / Misuse - Cyber [0761] @22/07/2016 14:32 (Sch4p4(6)

	Sch4p4(6) (Patrol group: GYMPIE, Court Dist./Div.: GYMPIE, Region: CENTRAL, District: WIDE BAY BURNETT, Division: GYMPIE, Stats area: 315103624)) (Occurrence Typ
Task:	T1603031746 [Init rpt - Closed] Due: 23/07/2016 15:08 #4032583 BUCHHOLZ, G. ->#4032583 BUCHHOLZ, G. [Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1601366042 Hacking / Misuse - Cyber [0761] @22/07/2016 14:32 (Sch4p4(6)
Author:	#4032583 BUCHHOLZ, G.
Report time:	22/07/2016 14:32
Entered by:	#4032583 BUCHHOLZ, G.
Entered time:	22/07/2016 15:08
Remarks:	Occurrence Type: Stealing from other specified buildings (including ATM transactions) (0835); Occurrence Address: 102 MARY ST, GYMPIE, QLD, 4570; Victim 1: Sch4p4(6) Suspect 1: Sch4p4(6)

Narrative:

MO

The complainant is the Generl Manager of Sch4p4 Sch4 which operates 24 branches across Queensland. The general manager is based in Sch4p4(6 but resides in Sch4p Sch The nominated suspect, an employee of Sch4p4 Sch4 resides in Sch4p and was employed as bank officer at the Sch4p Branch. Between January and July 2016, the suspect in his capacity as a Sch Sch4 has created a bogus account in his mother's name then created an electronic transfer of funds from an account held by S Sch4 Sch4p4(Various amounts of money during this period were transfered to this bogus account also with Sch4p4 Sch then transfered this money to an account in his name. The complainant can evidence the electronic transfer of monies.

GENERAL REPORT

Occurrence as per MO. On the 20th of July 2016 the complainant and the Sch4p4 Sch Regional Manager Sc Sch4p Sch4p confronted the suspect at the Sch4p Branch with the allegation where he made full admissions. His employment was subsequently terminated. Sch4p4 Sch have reimbursed the account holder Sch4p4(the amount of $6065.00 and seeking restitution for this amount. The complainant has provided a copy of Bank documants that have been scanned to the occurrence. Due to the complex nayure of the complkainant and the volume of the material provided perhaps the statement would be more appropriately obtained from a nominated investigator at Gympie CIB. SOC not required.

Details

Queensland Police Service

Report no.: QP1601529217
Occurrence Type: Hacking / Misuse - Cyber [0761]
Occurrence time: 09/08/2016 21:00 -
Reported time: 15/08/2016 12:10
Place of offence: Sch4p4(6) Patrol group: GOLD COAST CENTRAL, Court Dist./Div.: GOLD COAST, Region: SOUTH EASTERN, District: GOLD COAST, Division: SOUTHPORT, Stats area: 307153578)
Clearance status: Finalised
Summary: IDENTITY FRAUD - USE OF ANOTHER IDENTITY [0745]; Sch4p4(6) ; Victim/informant: Sch4p4(6) ; Suspect: Sch4p4(6) ***ADDENDUM 18/08/16 Occ type modified to Cyber Hacking Crime class***
Concluded summary:

Printed: 07/08/2017 10:05 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6)
   (Patrol group: GOLD COAST CENTRAL, Court Dist./Div.: GOLD COAST, Region: SOUTH EASTERN, District: GOLD COAST, Division: SOUTHPORT, Stats area: 307153578, NHW: SOUTHPORT 02)), Id #] / [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: IPSWICH METRO, Court Dist./Div.: IPSWICH, Region: SOUTHERN, District: IPSWICH, Division: IPSWICH, Stats area: 305253962) (Mobile telephone) Sch4p4(6)),] / Status: [Notice to appear (1b)]
   Cleared Unit: [TASKFORCE LATRO NORTH] / [03/09/2016]

Modus operandi:

1. Location: Dwelling. Subtype: House. Other behavior at scene: Other. Method of escape: Other. No. of offenders/suspects: One. Free text keywords: AT APPROXIMATELY 2100 HRS ON THE 09/08/2016 THE OFFENDER Sch4p4(6) Sch4 HAS PROCEEDED TO TRANSFER THE SUM OF $1900.00 FROM Sch4 Sch4p4(6 ACCOUNT WHILST ON THE COMPUTER AT Sch4p4(Sch4p4(6)Sch . SUSPECT Sch4 HAS UNLAWFULLY OBTAINED Sch4p4(6 BANK ACCOUNT DETAILS AND TRANSFERRED A SUM OF $1900.00 VIA INTERNER ANZ BANKING INTO HIS OWN ACCOUNT. .

Reports:

General report

Occurrence: QP1601529217 Hacking / Misuse - Cyber [0761] @15/08/2016 12:10 (Sch4p4(6) (Patrol group: GOLD COAST CENTRAL, Court Dist./Div.: GOLD COAST, Region: SOUTH EASTERN, District: GOLD COAST, Division: SOUTHPORT, Stats area: 3071535
Task: T1603392270 [Init rpt - Closed] Due: 16/08/2016 12:41 #4033317 TUIVANU, D. ->#4033317 TUIVANU, D. [Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1601529217 Hacking / Misuse - Cyber [0761] @15/08/2016 12:10 (Sch4p4(6)
Author: #4029247 BRENNAN, D.

Report time: 15/08/2016 12:10
Entered by: #4033317 TUIVANU, D.
Entered time: 15/08/2016 12:41
Remarks: IDENTITY FRAUD - USE OF ANOTHER IDENTITY [0745]; Sch4p4(6) ; Victim/informant: Sch4p4(6) 0Sch4p4(Suspect: Sch4p4(6)

Narrative:
MO

At approximately 2100 hrs on the 09/08/2016 the offender Sch4p4 Sch has proceeded to transfer the sum of $1900.00 from Sch Sch4p4(account whilst on the computer at Sch4p4(6) . Suspect Sch has unlawfully obtained Sch4p4(bank account details and transferred a sum of $1900.00 via interner ANZ banking into his own account.

GENERAL REPORT

At approximately 1210 hrs on the 15/08/2016 the victim attended the Southport Police station to report the fraudulent activity from Sch4 Sch has been a flat mate of Sch4p for 6 months. The suspect has moved his possessions from the nominated address around the nominated date of committing the offence. Sch4p was unsure of how Sch had obtained Sc bank account details. Sch4p will be attending Southport Police Station at 0800 hrs on the 16/08/2016 to provide a witness statement of the incident which will be scanned onto the occurrence after the witness statement has been taken. SOC are not required and wanted for questiong flag will be placed on suspect. Police will further speak with the ANZ crime unit telephone numeber Sch4p4(6) to obtain details of jonathan Sch4 bank account and which bank account Sc gained access to. Police also have a copy of the ANZ banking transaction which occurred on the 09/08/2016 which states that ANZ internet banking funds transfer Sch4p to Sch4p4 Sch4 The amount of aus dollars of $1900.00. At no time did Sch4p give permission for Sch to transfer those funds from Sc account to S account.

Details

Queensland Police Service

Report no.:	QP1601564315
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	22/09/2015 00:01 - 22/09/2015 23:59
Reported time:	29/09/2015 15:07
Place of offence:	Sch4p4(6) (Patrol group: GOLD COAST CENTRAL, Court Dist./Div.: GOLD COAST, Region: SOUTH EASTERN, District: GOLD COAST, Division: SOUTHPORT, Stats area: 307153578, Beat: ARUNDEL)
Clearance status:	Finalised
Operation name:	ACORN 1
ACORN #:	ARNFTHBDDYH
Summary:	HACKING / MISUSE - CYBER [0761] Occurrence address - Sch4p4(6) ; Informannt/Victim - Sch4p4(6)
Concluded summary:	

Printed: 07/08/2017 09:36 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Patrol group: INTERSTATE, Region: INTERSTATE, District: INTERSTATE, Division: INTERSTATE) (Land line) Sch4p4(6 Sch4p4(6) Id #:23270713] / [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: GOLD COAST CENTRAL, Court Dist./Div.: GOLD COAST, Region: SOUTH EASTERN, District: GOLD COAST, Division: SOUTHPORT, Stats area: 307153578, Beat: ARUNDEL) Sch4p4(6)] / Status: [Notice to appear (1b)]
   Cleared Unit: [SOUTHPORT CIB ((Land line) 0755714203)] / [02/05/2017]

Modus operandi:

1. Location: Dwelling. Subtype: House. Victim age: Female adult (over 18). Victim's prior actions: Unknown. Victim injuries sustained: No injury. Relationship to offender: Not known. Other behavior at scene: Other. Method of escape: Unknown. No. of offenders/suspects: One. Free text keywords: THE INFORMANT STATES A BENDIGO BANK ACCOUNT WAS OPENED ONLINE UNDER MY NAME WHICH I DID NOT AUTHORIZE. MY CENTRELINK PAYMENT DETAILS WERE CHANGED TO THE BANK ACCOUNT I DID NOT OPEN UNDER MY NAME TO WHERE I DID NOT RECEIVE MY BENEFITS..

Reports:

General report

Occurrence:	QP1601564315 Hacking / Misuse - Cyber [0761] @29/09/2015 15:07 Sch4p4(6) (Patrol group: GOLD COAST CENTRAL, Court Dist./Div.: GOLD COAST, Region: SOUTH EASTERN, District: GOLD COAST, Division: SOUTHPORT, Stats area: 30
Task:	T1603479640 [Init rpt - Closed] Due: 21/08/2016 15:12 #4035860 HILLMAN, A. ->#4035860 HILLMAN, A. [Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1601564315 Hacking / Misuse - Cyber [0761]

@29/09/2015 15:07 (Sch4p4(6)

Author: #4017822 HARTLEY, A.
Report time: 29/09/2015 15:07
Entered by: #4035860 HILLMAN, A.
Entered time: 20/08/2016 15:19
Remarks: HACKING / MISUSE - CYBER [0761] Occurrence address - Sch4p4(6); Informannt/Victim - Sch4p4(6)

Narrative:

MO

The informant states a Bendigo bank account was opened online under my name which i did not authorize. my Centrelink payment details were changed to the bank account i did not open under my name to where i did not receive my benefits.

GENERAL REPORT

Please detail to an investigator in the suspect area for follow up.

It is unknown how the suspect has been linked to this report. A contact of Sc from Bendigo bank crime department Sch4p4(has been provided.

Please refer to the attached external documents for full details of the ACORN referral and instructions concerning investigation obligations.

Investigators of cybercrime related matters should be aware of OPM 1.11 (Cybercrime reporting); 2.5.12 (Investigating cybercrime) and 2.6.8 (Specialist electronic and cybercrime investigations).

If investigations establish an offence location and it is in another jurisdiction (not Queensland) please ensure that all details of enquiries are recorded in the occurrence enquiry log. Change occurrence location to reflect the offence location and cancel the occurrence. Send a task to org unit 3343 (ACORN manager) for attention and referral of ACORN report to the responsible agency.

NOTE: There is no ACORN investigation unit within Fraud and Cyber Crime Group. Advice concerning investigating cybercrime can be obtained from the Cyber and Identity Crime Investigation Unit by internal email – SCC Cyber & ID Crime Investigation Unit

SOC not required

Details

Queensland Police Service

Report no.:	QP1601662301
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	05/08/2016 00:01 - 05/08/2016 23:59
Reported time:	24/08/2016 13:25
Place of offence:	SUBURB - COOLUM BEACH, COOLUM BEACH, QLD Australia 4573 (Patrol group: SUNSHINE COAST NORTHERN, Court Dist./Div.: MAROOCHYDORE, Region: CENTRAL, District: SUNSHINE COAST, Division: COOLUM, Stats area: 309106733)
Clearance status:	Finalised
Operation name:	ACORN 1
ACORN #:	ARN3EG7PJEB
Summary:	Hacking / Misuse - Cyber [0761]; SUBURB - COOLUM BEACH; Victim: Sch4p4 (6)
Concluded summary:	

Printed: 06/08/2017 21:06 by 4019283

Involved Offences:

1. [1810/ Referral Services] / [ ] / [ ]
   Victim: [ ] / [Non-Crime: Unsolved]
   Offender: [ ] / Status: [ ]
   Cleared Unit: [ ] / [ ]
2. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Patrol group: SUNSHINE COAST CENTRAL, Court Dist./Div.: MAROOCHYDORE, Region: CENTRAL, District: SUNSHINE COAST, Division: NAMBOUR, Stats area: 309056748, NHW: NAMBOUR 0] / [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: SUNSHINE COAST CENTRAL, Court Dist./Div.: MAROOCHYDORE, Region: CENTRAL, District: SUNSHINE COAST, Division: NAMBOUR, Stats area: 309056761)), Id #:Sch4p4 / Status: [Arrested (1a)]
   Cleared Unit: [NOOSA HEADS CIB (9 LANGURA ST, NOOSA HEADS, QLD Australia 4567 (Court Dist./Div.: MAROOCHYDORE, Region: CENTRAL, District: SUNSHINE COAST, Division: NOOSA HEADS, Stats area: 309056755) (Land line) 0754408167)] / [15/12/2016]

Modus operandi:

1. Location: Dwelling. Occupancy: Not known. Victim age: Female adult (over 18). Victim's prior actions: Unknown. Victim injuries sustained: No injury. Relationship to offender: Ex partner. Other behavior at scene: Unknown. Method of escape: Unknown. No. of offenders/suspects: Unknown. Free text keywords: THE SUSPECT HAS ACCESSED THE COMPLAINANTS CENTRELINK ACCOUNT AND DIVERTED $1,080 TO HIS OWN ACCOUNT. .

Reports:

General report

Occurrence:	QP1601662301 Hacking / Misuse - Cyber [0761] @24/08/2016 13:25 (SUBURB - COOLUM BEACH, COOLUM BEACH, QLD Australia 4573 (Patrol group: SUNSHINE COAST NORTHERN, Court Dist./Div.: MAROOCHYDORE, Region: CENTRAL, District:

Task:	SUNSHINE COAST, Division: COOLUM, St T1603704037 [Init rpt - Closed] Due: 04/09/2016 20:42 #4032055 SINN, C. ->#4032055 SINN, C. [Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1601662301 Hacking / Misuse - Cyber [0761] @24/08/2016 13:25 (SUBURB - COOLUM BEACH, CO
Author:	#4015931 SCOTT, P.
Report time:	24/08/2016 23:59
Entered by:	#4032055 SINN, C.
Entered time:	03/09/2016 21:01
Remarks:	Hacking / Misuse - Cyber [0761]; SUBURB - COOLUM BEACH; Victim: Sch4p4(6)

Narrative:

MO

The suspect has accessed the complainants Centrelink account and diverted $1,080 to his own account.

Officers Report

This is an ACORN referred report relating to an alleged cybercrime and which appears to have been committed in Qld.

Please refer to the attached external documents for full details of the ACORN referral.

Investigators of cybercrime related matters should be aware of OPM 1.11 (Cybercrime reporting); 2.5.12 (Investigating cybercrime) and 2.6.8 (Specialist electronic and cybercrime investigations).

The investigating officer is to notify the victim of the QP and ACORN number. **It is the investigating officer's responsibility to obtain all relevant information from the victim**. The ACORN system does not have the ability to transfer documents between agencies.

Investigations should also include any money laundering offences identified during the investigation.

Specialist advice, if required, should be sort through your local DEET or by emailing Cyber and Identity Crime Investigation Unit (SCC Cyber & ID Crime Investigation Unit). The engagement of CICIU to undertake investigation of ACORN or other matters is to be conducted through the State Crime Command engagement procedures as per OPM 2.7.1.

If investigations establish a suspect in another jurisdiction (not Queensland) please ensure that all details of enquiries are recorded on the occurrence. Change occurrence location to reflect the offence location and cancel the occurrence through PIR2. A review task will automatically be sent to org unit 3343 for attention.

Details

Queensland Police Service

Report no.:	QP1601736969
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	10/09/2016 00:00 - 10/09/2016 05:00
Reported time:	11/09/2016 13:00
Place of offence:	Sch4p4(6) (Patrol group: CENTENARY, Court Dist./Div.: BRISBANE/RICHLANDS, Region: BRISBANE, District: SOUTH BRISBANE, Division: MOUNT OMMANEY, Stats area: 305071167)
Clearance status:	Finalised
Operation name:	ACORN1
Misc. file:	QP1601742440
ACORN #:	ARNJY38G837
Summary:	Cyber Crime - Computer Hacking - Victim - Sch4p4(6) , Suspect - Sch4p4(6) , Location - Sch4p4(6)
Concluded summary:	

Printed: 07/08/2017 07:33 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6)), Id #:Sch4p4(6
   DL:QLD:Sch4p4(6) / [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: BAYSIDE, Court Dist./Div.: BRISBANE/WYNNUM, Region: BRISBANE, District: SOUTH BRISBANE, Division: WYNNUM, Stats area: 305111571, Beat: TINGALPA, NHW: WYNNU] / Status: [Arrested (1a)]
   Cleared Unit: [INALA STATION (POLICE - INALA POLICE SHOPFRONT, INALA, QLD Australia 4077 (Patrol group: CENTENARY, Court Dist./Div.: BRISBANE/RICHLANDS, Region: BRISBANE, District: SOUTH BRISBANE, Division: INALA, Stats area: 305071288, Beat: INALA) (Land line) 07373755] / [07/10/2016]

Modus operandi:

1. Location: Dwelling. Subtype: House. Victim age: Female adult (over 18). Victim's prior actions: At home. Victim injuries sustained: No injury. Relationship to offender: Acquaintance. Method of escape: Unknown. No. of offenders/suspects: One. Free text keywords: SUSPECT HAS OBTAINED VICTIMS IPHONE AND HAS “HACKED” INTO Sch PHONE BY UNKNOWN MEANS, BYPASSING THE PASSCODE AND GAINING ACCESS TO Sch IPHONE PROPER. SUSPECT HAS THEN ACCESSED Sch PHOTOGRAPHS WITHIN THE IPHONE AND HAS LOCATED 38 IMAGES OF THE VICTIM AND 1 VIDEO WHICH Sc HAS THEN FORWARDED TO Sc OWN MOBILE BY INSTANT MESSAGING. THESE PHOTOGRAPHS ARE MAINLY INDECENT PHOTOGRAPHS OF THE VICTIM IN VARIOUS POSES WHERE Sch IS DEPICTED NAKED OR SEMI NAKED. THESE IMAGES HAVE TAKEN FROM THE PHONE WITHOUT THE PERMISSION OF THE VICTIM..

Reports:

General report

Occurrence:	QP1601736969 Hacking / Misuse - Cyber [0761] @11/09/2016 13:00 (Sch4p4(6) (Patrol group: CENTENARY, Court

	Dist./Div.: BRISBANE/RICHLANDS, Region: BRISBANE, District: SOUTH BRISBANE, Division: MOUNT OMMANEY, Stats area: 305
Task:	T1603883648 [Init rpt - Closed] Due: 15/09/2016 22:19 #4025037 ISSANCHON, R. ->#4025037 ISSANCHON, R. [Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1601736969 Hacking / Misuse - Cyber [0761] @11/09/2016 13:00 Sch4p4(6)
Author:	#4008063 TOLSHER, D.
Report time:	11/09/2016 13:00
Entered by:	#4025037 ISSANCHON, R.
Entered time:	14/09/2016 22:23
Remarks:	Cyber Crime - Computer Hacking - Victim - Sch4p4(6) Suspect - Sch4p4(6) , Location - Sch4p4(6)

Narrative:

MO

Suspect has obtained victims iphone and has "hacked" into Sc phone by unknown means, bypassing the passcode and gaining access to Sc iphone proper. Suspect has then accessed Sc photographs within the iphone and has located 38 images of the victim and 1 video which Sc has then forwarded to Sc own mobile by instant messaging. These photographs are mainly indecent photographs of the victim in various poses where Sc is depicted naked or semi naked. These images have taken from the phone without the permission of the victim.

General Report

On the evening of Friday the Sc /09/2016 the victim attended to the Sch4p4(6) and met up with Sc friends for a night of drinking and dancing. Whilst there Sc met a Sch4 person who introduced Sch4p4 at Sch4p This Sch4 person was dressed in a Sch4p4(6) and stated that Sc was Sch4p4(6) that night. The victim has exchanged phone numbers with the suspect and during the course of the evening has texted Sch a number of times. The victim has had further conversations with Sch later in the evening where they made arrangements to leave together. The suspect has driven the victim to Sc address at Sch4p4(6) . The victim has asked the suspect to stay the night but has made it clear to Sch that Sc didn't want any sexual interaction. The suspect has agreed to come inside, the victim has stated Sc sensed Sc demeanour changed when Sc realised there were other persons in the house, namely the victim's Sch4p4(and Sch4p4(6) . Sch stated that Sc became agitated and stated Sc wanted to leave. Victim has then gone to the bathroom and left Sch alone in Sc room with Sc mobile phone whilst Sc was in the bathroom. Upon exiting the bathroom Sc hopped into bed, suspect was talking to the victim and Sc started to fall asleep. Victim stated Sc soon fell asleep and the suspect has left the dwelling. Enquiries with the housemate of the victim Sch4p4(6) stated Sc believes Sc heard the suspect leave at around 0400 to the best of Sc recollection. Later that morning when the victim woke up Sc found that the suspect had gone. The victim has later checked Sc laptop computer and upon doing so saw there was a notification on Sc computer showing Sc had sent messages to a phone number which she recognised as being the suspects number and thought this to be unusual and checked her mobile phone. At this time she found that all the messages Sc had sent to the suspect earlier had been deleted and found this strange, Sc checked the laptop again and checked Sc messages on the laptop and saw that a number of photographs "indecent" of Sch4p had been sent from Sc mobile phone to

the suspects mobile phone while Sc was asleep in Sc room. The photographs total 38 photographs and 1 video. The victim has realised what has gone on and has later that day contacted the suspect who denied having access to the mobile phone and sending the photographs to Sch4p4(The victim has become concerned that the photographs could be shared with other persons or on the internet and has subsequently attended Inala Station on SS/09/2016 and made a complaint regarding this matter. Police have conducted a check of the mobile number which the suspect provided to Sc as Sc mobile (Sch4p4(6) This mobile number comes up to a Sch4 person by the name Sch4p4(6) It is obvious that Sch4p4(has provided a false name to the victim upon their meeting. Sch3(10)(1)(f)

[redacted]

***

Details

Queensland Police Service

Report no.:	QP1602106296
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	20/10/2016 10:47 -
Reported time:	10/11/2016 15:33
Place of offence:	Sch4p4(6) (Patrol group: WEST GATEWAY, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: STAFFORD, Stats area: 305031244)
Clearance status:	Finalised
Operation name:	ACORN 1
ACORN #:	ARN6BRGA6B6
Summary:	Hacking / Misuse - Cyber [0761] Sch4p4(6) . Victim: Sch4p4(6) Sch4p4(6) .
Concluded summary:	

Printed: 07/08/2017 06:18 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, Stats area: 305011143) (GNAF- Retired as of Feb2010;))] / [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: WEST GATEWAY, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: STAFFORD, Stats area: 305031244)), Id #:Sch4p4(6) :Sch4p / Status: [Notice to appear (1b)]
   Cleared Unit: [HI-TECH CRIME INVESTIGATION UNIT (POLICE - ROMA ST POLICE STATION, ROMA ST, BRISBANE CITY, QLD Australia 4000 (Patrol group: CITY CENTRAL, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, Stats area:] / [19/03/2017]

Modus operandi:

1. Location: Commercial. Subtype: Office. Occupancy: Not known. Other behavior at scene: Other. Method of escape: Unknown. No. of offenders/suspects: Unknown. Computer hacking method: Access/interfere computer systems. Free text keywords: ON THE NOMINATED OFFENCE DATE Sch4p4(6) IT SECURITY TEAM DETECTED UNUSUAL ACTIVITY, SPECIFICALLY A NUMBER OF ATTEMPTED LOGIN'S VIA Sch4p4(6) REMOTE LOG-IN SYSTEM (Sch4p4 BEING MADE UNDER A FORMER EMPLOYEE'S 'USERID'; AND ALSO A NUMBER OF FAILED REMOTE LOGIN ATTEMPTS VIA Sch4p USING A NUMBER OF CURRENT EMPLOYEE USERID'S. NO ACCESS TO THE RESTRICTED COMPUTER WAS GAINED AS ALL ATTEMPTS TO ACCESS THE FORMER AND CURRENT EMPLOYEE ACCOUNTS FAILED. NO DETRIMENT, GAIN, BENEFIT OR DAMAGE WAS MADE AS A RESULT OF THE ATTEMPTED USE OF THE Sch4p4(COMPUTER SYSTEM..

Reports:

General report

Occurrence:	QP1602106296 Hacking / Misuse - Cyber [0761] @10/11/2016 15:33 (Sch4p4(6) (Patrol group: WEST GATEWAY, Court

Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: STAFFORD, Stats area: 3050312

Task: T1604765450 [Init rpt - Closed] Due: 11/11/2016 17:27 #4029854 GRUBBA, M. ->#4029854 GRUBBA, M. [Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1602106296 Hacking / Misuse - Cyber [0761] @10/11/2016 15:33 (Sch4p4(6)

Author: #4010504 NIKOLA, C.

Report time: 10/11/2016 15:33

Entered by: #4029854 GRUBBA, M.

Entered time: 10/11/2016 17:31

Remarks: Hacking / Misuse - Cyber [0761] Sch4p4(6) .
Victim: Sch4p4(6) .

Narrative:

MO

On the nominated offence date Sch4p IT Security team detected unusual activity, specifically a number of attempted login's via Sch4p remote log-in system (Sch being made under a former employee's 'userid'; and also a number of failed remote login attempts via Sch using a number of current employee userid's. No access to the restricted computer was gained as all attempts to access the former and current employee accounts failed. No detriment, gain, benefit or damage was made as a result of the attempted use of the Sch4 computer system.

GENERAL REPORT

On Thursday S /10/2016, Sch4p central security monitoring platform (Sch detected a former employee's account attempting to log in as well as multiple failed remote login attempts via the Sch Access Gateway. The two alarms that triggered are: (1) Former Employee Login - detecting unauthorised access attempts with an account that has been disabled once an employee is terminated (2) Multi-user Password Guessing from External IP - multiple accounts having failed login attempts from a single, external source

These events were assessed as a Security Incident and an investigation was immediately conducted by Sch4p

Initial investigations confirmed that these events (former member login access attempts and multiple failed current member access attempts) were from a single Sch4p4(6) . Further is that all the users with access attempts are from the Sch4p4(6) , mostly accounts being Sch4 S Advisors.

None of the logins attempted were successful however the activity appeared to be targeted.

Correct Process for log-in:

1. Enter username. Six letters, the first two letters are the first two letters of the users name, the last four letters of the username are the first four letters of the users surname.
2. Enter Password. Same password used by user to log-on when in Sch4 office.
3. Sch4p4(6)

Failed Former Member Attempted Login's

Initial investigations were conducted into the former user 'Sch4p attempting to login via Sch This triggered an alarm in the system as this was immediately identified as a Sch4p4(6) . There were three (3) separate attempted logins under the former user name of 'Sch4p The former employee login account of 'Sch4p belongs to former Sch4p4(6) . Sch4 employee account names are made up of a combination of the first two letters of an employee's first name and the first four letters of the surname. In this instance the employee name of Sch4p4(6) '. Sch4 records indicate that a search for Sch4p4(6) Sch4p4(6) . The user id remained the same however. Sch4 confirmed that Sch4p Sch4p4 was terminated on Sch4p4(

Failed Current Member Attempted Login's

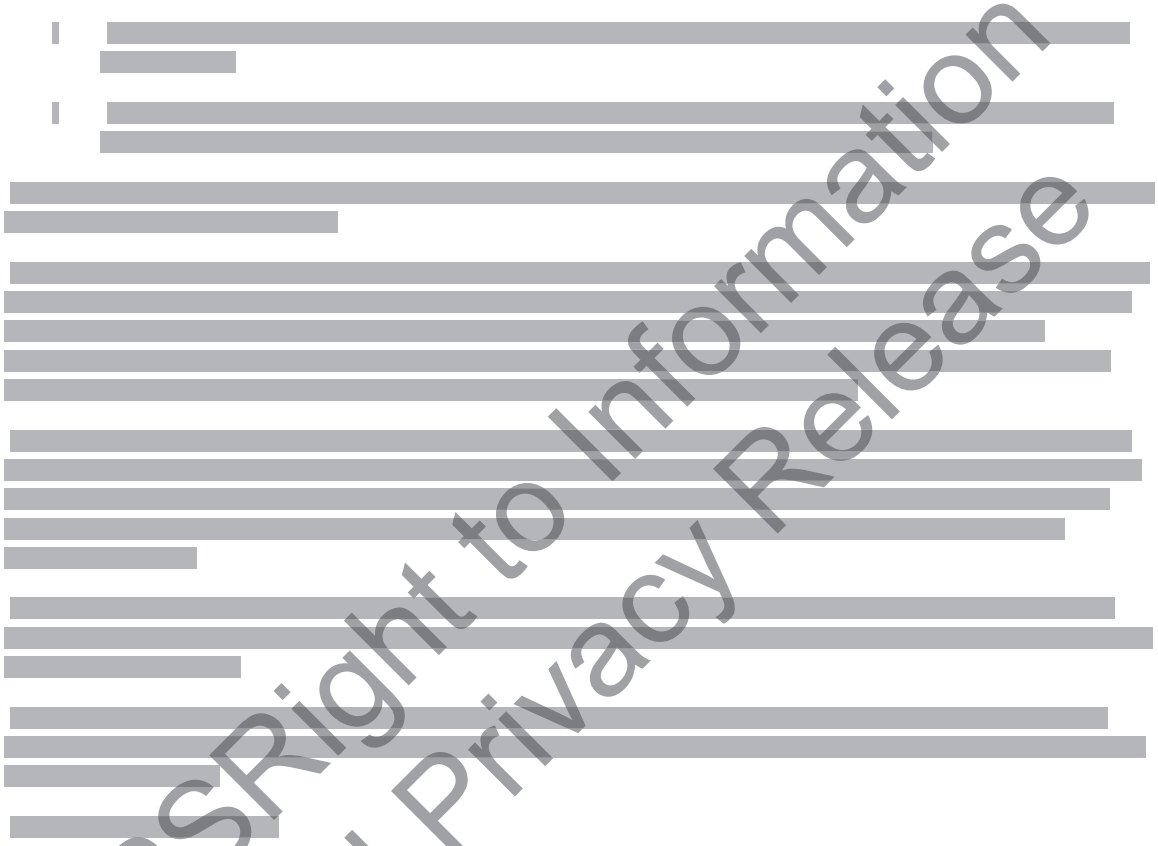
There are fourteen (14) separate attempted logins using current employee userid's and passwords. Eleven of those separate attempted logins relate to the userid of current employee Sch4p4(6) . Further analysis confirms the same source Sch4p4(6) address tried and failed to log in to the Sch4 account was ALSO used to attempt to login on 14 separate occasions to these active member accounts. Investigations confirm that Multi-user Password Guessing also occurred for this same source IP address for the current member accounts. All 14 access attempts failed.

It is relevant to the investigation that shortly after these attempted login attempts have occurred (and failed) a call has been received by the Sch4 IT Help Desk operator Sch4p4(6) from a Sch4 who identified Sch4 as Sch4 Sch4 The Sch4 has stated that Sc cannot remotely login to the network. Sch has then attempted to assist this

person in logging onto Sch4 Sch4 account (based on S understanding that S was speaking to Sch4 Sch4 However all attempts to do this were unsuccessful by Sch who then advised the caller that S would continue to try and rectify the issue and that since this would take some time, S would call back. S was provided a mobile phone number by the caller of Sch4p4(6) . Approximately 20 minutes later, Sch attempted to call the person on the mobile number provided but was unsuccessful. This person then called the Service Desk again, returning Sch4p Sch4 call. This voice call was recorded by Sch4p

At the start of business on Friday 21 October 2016, actual current employee Sch4 Sch called the IT Service Desk advising there were issues with her remote access. Sch4p identity was confirmed by the IT Service Desk via security questions, however when asked if Sc had called previously, Sc confirmed Sc had not raised this issue yet. This voice call was also recorded by Sch4p At this time it was ascertained that this was security issue was inextricably linked to the attempted userid breaches as it appears to confirm that the previous caller purporting to be Sch4 is likely to be a different person.

Sch4p4(6), Sch3(10)(1)(f)



This is an ACORN referred report relating to an alleged cybercrime and which appears to have been committed in Queensland.

Please refer to the attached external documents for full details of the ACORN referral.

Investigators of cybercrime related matters should be aware of OPM 1.11 (Cybercrime reporting); 2.5.12 (Investigating cybercrime) and 2.6.8 (Specialist electronic and cybercrime investigations).

The investigating officer is to notify the victim of the QP and ACORN number. It is the investigating officer's responsibility to obtain all relevant information from the victim. The ACORN system does not have the ability to transfer documents between agencies.

Investigations should also include any money laundering offences identified during the investigation.

Specialist advice, if required, should be sort through your local DEET or by emailing Cyber and Identity Crime Investigation Unit (SCC Cyber & ID Crime Investigation Unit). The engagement of CICIU to undertake investigation of ACORN or other matters is to be conducted through the State Crime Command engagement procedures as per OPM 2.7.1.

If investigations establish a suspect in another jurisdiction (not Queensland) please ensure that all details of enquiries are recorded on the occurrence. Change occurrence location to reflect the offence location and cancel the occurrence through PIR2. A review task will automatically be sent to org unit 3343 for attention.

Details

Queensland Police Service

Report no.:	QP1700186768
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	27/01/2017 00:01 - 27/01/2017 23:59
Reported time:	30/01/2017 17:58
Place of offence:	Sch4p4(6) (Patrol group: CITY CENTRAL, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, Stats area: 305011143) (GNAF-Retired as of Feb2010;)
Clearance status:	Finalised
Operation name:	ACORN 1
ACORN #:	ARNHJRJ3KRJ
Summary:	Hacking / Misuse - Cyber [0761]- Occurrence Address; Sch4p4(6) Informant; Sch4p4(6) - Victim; Sch4p4(6) - Suspect; Sch4p4(6)
Concluded summary:	

Printed: 07/08/2017 10:13 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, Stats area: 305011143) (GNAF- Retired as of Feb201] / [Crime: Solved]
   Offender: [ ] / Status: [Arrested (1a)]
   Cleared Unit: [HI-TECH CRIME INVESTIGATION UNIT (POLICE - ROMA ST POLICE STATION, ROMA ST, BRISBANE CITY, QLD Australia 4000 (Patrol group: CITY CENTRAL, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, Stats area:] / [11/03/2017]

Modus operandi:

1. Location: Commercial. Subtype: Office. Other behavior at scene: Other. Method of escape: Other. No. of offenders/suspects: One. Computer hacking method: Access/interfere computer systems; Access/interfere data; Access/interfere programs. Free text keywords: IT IS ALLEGED THAT SUSPECT IN THIS INSTANCE HAS HACKED THE COMPLAINANT'S BUSINESS RESERVATION DATABASE AND DELETED AND CHANGED INFORMATION AS WELL AS CHANGING PASSWORDS TO REMOVE THE COMPLAINANTS ACCESS. COMPLAINANT BELIEVES THEY KNOW SUSPECT AS A PAST EMPLOYEE..

Reports:

General report

Occurrence:	QP1700186768 Hacking / Misuse - Cyber [0761] @30/01/2017 17:58 (Sch4p4(6) (Patrol group: CITY CENTRAL, Court Dist./Div.: BRISBANE/CENTRAL, Region: BRISBANE, District: NORTH BRISBANE, Division: BRISBANE CITY, Stats area:
Task:	T1700440363 [Init rpt - Closed] Due: 01/02/2017 08:46 #4035870 SMITH, C. ->#4035870 SMITH, C. [Low] QPS Investigative Task Workflow Initial Report Task and Start

Point QP1700186768 Hacking / Misuse - Cyber [0761]
@30/01/2017 17:58 (Sch4p4(6)
Author: #4033294 CHRZESCIJANSKI, J.
Report time: 30/01/2017 17:58
Entered by: #4035870 SMITH, C.
Entered time: 31/01/2017 08:52
Remarks: Hacking / Misuse - Cyber [0761]- Occurrence Address; S
Sch4p4(6) - Informant; Sch4p4(6)
- Victim; Sch4p4(6) -
Suspect; Sch4p4(6)

Narrative:

MO

It is alleged that suspect in this instance has hacked the complainant's business reservation database and deleted and changed information as well as changing passwords to remove the complainants access. Complainant believes they know suspect as a past employee.

This is an ACORN referred report relating to an alleged cybercrime and which appears to have been committed in Queensland.

Please refer to the attached external documents for full details of the ACORN referral.

Investigators of cybercrime related matters should be aware of OPM 1.11 (Cybercrime reporting); 2.5.12(Investigating cybercrime) and 2.6.8 (Specialist electronic and cybercrime investigations).

The investigating officer is to notify the victim of the QP and ACORN number. **It is the investigating officer's responsibility to obtain all relevant information from the victim**. The ACORN system does not have the ability to transfer documents between agencies.

Investigations should also include any money laundering offences identified during the investigation.

Specialist advice, if required, should be sort through your local DEET or by emailing Cyber and Identity Crime Investigation Unit (SCC Cyber & ID Crime Investigation Unit). The engagement of CICIU to undertake investigation of ACORN or other matters is to be conducted through the State Crime Command engagement procedures as per OPM 2.7.1.

If investigations establish the offence has occurred in another jurisdiction (not Queensland) please ensure that all details of enquiries are recorded on the occurrence. Change occurrence location to reflect the offence location and cancel the occurrence through PIR2.

A report is then to be prepared and forwarded through the chain as outlined in OPM 1.11.2 – interstate offences.

Details

Queensland Police Service

Report no.:	QP1700233796
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	07/01/2017 09:00 -
Reported time:	27/01/2017 13:37
Place of offence:	Sch4p4(6) (Patrol group: LOGAN WEST, Court Dist./Div.: BEENLEIGH, Region: SOUTH EASTERN, District: LOGAN, Division: CRESTMEAD, Stats area: 305304623, NHW: CRESTMEAD 02)
Clearance status:	Finalised
Operation name:	ACORN 1
ACORN #:	ARNPDPB84JJ
Summary:	Hacking/ Misuse - Sch4p4(6) . Victim is Sch4p4(6) . Offender is Sch4p4(6) .
Concluded summary:	

Printed: 07/08/2017 09:47 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: [Sch4p4(6) (Patrol group: LOGAN CENTRAL AND NORTH, Court Dist./Div.: BEENLEIGH, Region: SOUTH EASTERN, District: LOGAN, Division: LOGAN CENTRAL, Stats area: 305304612)), Id #:Sch4p4(/ [Crime: Solved]
   Offender: [Sch4p4(6) (Patrol group: SUNSHINE COAST CENTRAL, Court Dist./Div.: MAROOCHYDORE, Region: CENTRAL, District: SUNSHINE COAST, Division: MAROOCHYDORE, Stats area: 309056738)), Id] / Status: [Arrested (1a)]
   Cleared Unit: [PACIFIC PINES NEIGHBOURHOOD POLICE BEAT (33 SHEFFIELD CCT, PACIFIC PINES, QLD Australia 4211 (Patrol group: GOLD COAST NORTHERN, Court Dist./Div.: GOLD COAST, Region: SOUTH EASTERN, District: GOLD COAST, Division: NERANG, Stats area: 307153572, Beat: PACI] / [07/02/2017]

Modus operandi:

1. Location: Dwelling. Subtype: House. Victim age: Female young person (under 18). Relationship to offender: Acquaintance. No. of offenders/suspects: One. Free text keywords: ON THE NOMINATED DATE AND TIME, THE VICTIM USED THE OFFENDER'S TELEPHONE TO ACCESS HER CENTRELINK ACCOUNT. THE VICTIM HAS FORGOTTEN TO LOG OFF AND THE OFFENDER HAS THEN GONE INTO THE CENTRELINK ACCOUNT, CHANGED THE BANK ACCOUNT DETAILS TO THE OFFENDER'S OWN COMMONWEALTH ACCOUNT AND RECEIVED $761 ON THE VICTIM'S NEXT PAYMENT DATE..

Reports:

General report

Occurrence:	QP1700233796 Hacking / Misuse - Cyber [0761] @27/01/2017 13:37 Sch4p4(6) (Patrol group: LOGAN WEST, Court Dist./Div.: BEENLEIGH, Region: SOUTH EASTERN, District: LOGAN, Division: CRESTMEAD, Stats area: 305304623, NHW: CRE
Task:	T1700559334 [Init rpt - Closed] Due: 08/02/2017 11:39 #5028964 LOCK, R. ->#5028964 LOCK, R. [Low] QPS

Investigative Task Workflow Initial Report Task and Start Point QP1700233796 Hacking / Misuse - Cyber [0761] @27/01/2017 13:37 (Sch4p4(6)

Author: #4017063 WILLIAMS, R.
Report time: 27/01/2017 13:37
Entered by: #5028964 LOCK, R.
Entered time: 07/02/2017 11:46
Remarks: Hacking/ Misuse - Cyber at Sch4p4(6) .
Victim is Sch4p4(6) . Offender is

Narrative:
MO

On the nominated date and time, the victim used the offender's telephone to access her Centrelink account. The victim has forgotten to log off and the offender has then gone into the Centrelink account, changed the bank account details to the offender's own Commonwealth account and received $761 on the victim's next payment date.

GENERAL REPORT

On the S /2/17, offender has attended the Nerang Police Station with a support person . Initially the offender made full admissions

Offender released on bail conditions.

SOC not required.

ACORN report ARNPDPB84JJ.

Details

Queensland Police Service

Report no.:	QP1700716120
Occurrence Type:	Hacking / Misuse - Cyber [0761]
Occurrence time:	18/09/2015 08:00 - 18/09/2015 17:00
Reported time:	24/04/2017 14:24
Place of offence:	Sch4p4(6) (Patrol group: TOWNSVILLE SOUTHERN, Court Dist./Div.: TOWNSVILLE, Region: NORTHERN, District: TOWNSVILLE, Division: MUNDINGBURRA, Stats area: 345057001, Beat: STOCKLAND TOWNSVILLE, NHW: MUNDINGBURRA 06
Clearance status:	Finalised
ACORN #:	ACORN1
Summary:	Hacking / Misuse - Cyber. Occurrence Address: Sch4p4(6)
Concluded summary:	

Printed: 07/08/2017 09:41 by 4019283

Involved Offences:

1. [0761/ Hacking / Misuse - Cyber] / [Completed offence] / [1]
   Victim: Sch4p4(6)

Modus operandi:

1. Location: Commercial. Subtype: Bank. Occupancy: Not known. Victim age: Male adult (over 18). Victim's prior actions: Unknown. Victim injuries sustained: No injury. Relationship to offender: Stranger. Other behavior at scene: Other. Method of escape: Unknown. No. of offenders/suspects: One. Communication device: Email. Free text keywords: AN UNKNOWN OFFENDER HAS HACKED INTO EMAIL OF ONE OF THE VICTIMS WORK SUPPLIERS. SUSPECT CREATED FICTITIOUS (BUT SIMILAR) EMAIL ADDRESSES TO HIS EMAIL AS WELL AS THE SUPPLIER'S EMAIL AND COMMUNICATED BETWEEN BOTH VICTIM AND SUPPLIER, PRETENDING TO BE ONE OF US IN CONVERSATIONS WITH THE OTHER. THE SUSPECT, PRETENDING TO BE THE SUPPLIER, ADVISED DIFFERENT BANK DETAILS FOR A PAYMENT THAT I WAS INTENDING TO MAKE TO MY SUPPLIER. THE VICTIM WAS OVERSEAS ON HOLIDAY AT THE TIME AND WAS UNABLE TO PHONE THE SUPPLIER TO CONFIRM THE CHANGE IN BANK DETAILS. THE VICTIM MADE A PAYMENT OF $11,000 TO THE BANK ACCOUNT PROVIDED BY THE SUSPECT, AS I DID NOT REALISE THE SUSPECT HAD HACKED INTO THE EMAIL/HAD CREATED FALSE EMAIL ADDRESSES. ON RETURN TO AUSTRALIA IDENTIFIED THE FRAUD..

Reports:

General report

Occurrence: QP1700716120 Hacking / Misuse - Cyber [0761]
Sch4p4(6)

	Sch4p4(6) (Patrol group: TOWNSVILLE SOUTHERN, Court Dist./Div.: TOWNSVILLE, Region: NORTHERN, District: TOWNSVILLE, Division: MUNDINGBURRA, Stats a
Task:	T1701724154 [Init rpt - Closed] Due: 25/04/2017 15:26 #4027152 MULLER, C. ->#4027152 MULLER, C. [Low] QPS Investigative Task Workflow Initial Report Task and Start Point QP1700716120 Hacking / Misuse - Cyber [0761] @24/04/2017 14:24 Sch4p4(6)
Author:	#4011085 KIRKHAM, A.
Report time:	24/04/2017 14:24
Entered by:	#4027152 MULLER, C.
Entered time:	24/04/2017 15:31
Remarks:	Hacking / Misuse - Cyber. Occurrence Address: Sch4p 4(6) .

Narrative:

MO

An unknown offender has hacked into email of one of the victims work suppliers. Suspect created fictitious (but similar) email addresses to his email as well as the supplier's email and communicated between both victim and supplier, pretending to be one of us in conversations with the other.

The suspect, pretending to be the supplier, advised different bank details for a payment that I was intending to make to my supplier. The victim was overseas on holiday at the time and was unable to phone the supplier to confirm the change in bank details.

The victim made a payment of $11,000 to the bank account provided by the suspect, as I did not realise the suspect had hacked into the email/had created false email addresses.

On return to Australia identified the fraud.

GENERAL REPORT

Sch4p4(6) who is a suppliers for the victim company had sent an email and invoice for $11, 000 to the victim company from email address is Sch4p4(6) with Commonwealth Bank of Australia account details Sch4p4(6) .

On Tuesday the S t of September 2015 they received another email from a person posing as Sch4p4(6) they requested that money now be sent to a new bank account Sch4p4(6)

The victim has then instructed Sch4 to transfer the money to the new account.

On Wednesday the Sch of September 2015 Sch4 has transferred $11, 000 to Sch4p4(6) from there Sch4p4(6) t Building Society account name; Sch4p4(6)

Checks of account Sch4p4(6) show that the account belongs to Sch4p4(6) . Check of this account show the money going into the account on the 16th of September 2015.

On Friday the 18th of September 2015 Sch4p4(6) transferred $7000 to his Commonwealth Bank of Australia account Sch4p4(6) . He also made a cash withdrawal of $4000 at the Sch4p4(6) Credit Union Australia on the same day.

On Friday the 18th of September 2015 the victim discovered the fraud and report the matter to the New South Wales Police. As a result they contacted Credit Union Australia who put a hold on the suspect's bank accounts and also notified the Commonwealth Bank who also recovered the $7000 that had been transferred into the defendant's account. However the $4000 was never recovered.

At no time was the money meant to be sent to suspect and he did not have permission to use this money in anyway

This is an ACORN referred report relating to an alleged cybercrime.

Sch3(10)(1)(f) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

SOC not required.