SILICON KNIGHT COMPUTERS

SILICON KNIGHT COMPUTERS
50 Narangga Terrace
Moonta Bay
SA, 5558

Phone ([redacted]
Mobile [redacted]

www [redacted]

ABN : 34 352 318 409

PHOTOGRAPH - WHATSAPP APP
TOSHIBA LAPTOP - PURCHASED 2009.
PREVIOUS COMPUTER SYSTEM.

RECEIPT

Receipt # SO-001970
Date 4/06/2020

CLIENT DETAILS

[redacted]

$100.00
TOTAL PAID

ITEM	DESCRIPTION	QUANTITY	UNIT PRICE	SUB-TOTAL
*	Perform virus, malware, adware, crapware and trace removal. Reset browser homepages, search engines, and extensions. Perform system and registry clean. Install latest Windows online updates. - Warranty : NIL	1	$100.00	$100.00

* [redacted] Toshiba Satellite L500 laptop

[redacted] computer cleaned of virus/malware infections. Performed cleanup as described [redacted] Removed Slimware Driver Update crapware.

[redacted]

* [redacted] * - 135,936 MALWARE.

[redacted]

SUB-TOTAL	$100.00
TOTAL	$100.00
PAID	$100.00

Note : All sales are subject to our terms and conditions which are available upon request.

Ticket#621581/ New message via your website, from [redacted] Has been updated

Pit Stop Technologies <[redacted]> * 6/07/2020

To: [redacted] <jacqueline.c[redacted]>

--REPLY above this line to respond--

Hi Jacqueline,

Sorry to hear, so many scammers and hackers are in full force at the moment. I can have a tech available tomorrow to assist you, you may need us to check other accounts and apply additional security although you have started down the tight path. If they are not fully locked out they will continue to hack you further so the sooner we get started the better.

It may be in your best interest to come in as soon as you can. Depending on how far the hackers have gone and the steps we need to take to prevent them from having any further access can take anywhere from 2 - 6 hours. Our hourly rates are $150 + GST.

Let me know when you would like to come in.

Thanks

Helene Martin

98 Port Road | Kadina, SA 5554
Phone [redacted]

website | email

96 Hacking attempts in 2 days of new computer system Business accounts and new IP Address. SPECIFIED TARGETING OF THE INDIVIDUAL Knowledge under the act of Illegal surveillance of purchase of new computer system and newly created business accounts - IN CONNECTION TO TECSIRA REPORT FRAUDULENT ACTIVITY NON BUSINESS ACCOUNT 2020 - JOSHUA ADAMS, KADINA

Service Ticket #621581 - Jacqueline Pearce - Email Hack - 0400404658

Pit Stop Technologies [redacted]

Thu 9/07/2020 9:24 AM

To: [redacted]

Hello Jacqueline,

Service Ticket # 621581, has been completed. We hope that you are satisfied with the service provided. If you do not believe this ticket has been complete or have concerns, please respond to this email so we can address your queries.

Thank you,
Pit Stop Technologies Team
[redacted]
www.pit.net.au

PIT STOP TECHNOLOGIES
KEEPING YOUR IT ON TRACK

Ticket #: 621581 **Status:** Complete

Summary: Jacqueline Pearce - Email Hack - 0400404658

Service Record #621581
Summary: Jacqueline Pearce - Email Hack - 0400404658
Company: Jacqueline Pearce
Contact: Jacqueline Pearce
Phone: 0400-404-658

CREATED NEW ACCOUNTS - UPGRADED SECURITY SYSTEMS
2 STEP VERIFICATION FOLLOWING NEWLY CREATED
TELSTRA BUSINESS ACCOUNT / NEW PHONE NUMBER.

NEWLY FORMED BUSINESS ACCOUNTS, SECURITY SYSTEMS · NEW COMP
SYSTEM AND BUSINESS EMAIL ACCOUNTS.
NEWLY FORMED PERSONAL EMAIL ACCOUNT - MICROSOFT - GMAIL

Pitstop Technologies
Port Road, Kadina
SA 5554

JC INNOVATIONS
[redacted]

CONFIDENTIAL

Manager, Pitstop Technologies, Kadina

28th September 2020 · FOLLOWING NEW SET UP OF COMPUTER SYSTEM

Hacking of computer system
Escalated to Specific targeting of an individual - Not random

Suspected start of hacking of newly purchased systems and newly formed accounts, setup by Brennan of Pitstop Technologies, Kadina SA 5554 - Phone - Apple IPad - Computer System

Identified in Telstra, Kadina 2 weeks previous to date on top of this letter - sighted by Joshua Adams, Telstra Business Consultant - restricted access on newly formed business account, JC INNOVATIONS
Event: All internet supported apps stopped working, including emails and Netbanking - Informed by Joshua Adams that the security systems on my phone were blocking the access and functions of the internet supported apps. Advised to take my phone to an IT Specialist to sort out the issue as he could not assist me and did not have the knowledge to fix the problem. I stepped out of the Telstra store, Kadina to take my phone to Pitstop Technologies for assistance on the issue and the phone suddenly started to work and all internet functions began to work again as I stood outside on the footpath in front of the store.

1 week later
Event: Logged into my newly formed goggle account on my Apple IPad and received notification via email of a suspicious login attempt. I received a phone call from Matthew, Pitstop Technologies the next day asking me about this suspicious login as he had viewed the email notification through remote access of Brennan concerning the security measures he had installed because of the previous hacking of my previous system. I informed Matthew that it was me logging in on my IPad.

2 days later
Event : I received notification via my email informing me that there had been a suspicious login on my Netflix account and to change my password.
I logged into my goggle account on my IPad to check the account for suspicious activity. It reported in my account that I was logged in with a Mac computer not my Apple IPad. I do not own a Mac computer or have I ever owned a Mac computer.

2 days later:
Event : New computer system showed connected to an internet modem, the internet working, the modem number exact specified number of my internet modem - my internet modem was not turned on at the time and no internet modem was turned on in the house at this time. There was no access to allow the internet system to be working.

New computer system recently purchased and setup and installed security systems by Brennan, Pitstop Technologies, Kadina - 96 attempts of hacking in the first 3 days of turning on the new system - Report McAfee security - IP Addresses attempting hacking copied and given to Brennan, Pitstop Technologies, Kadina

Apple IPad - Internet system - wireless modem

Event: When connected to the internet on my Apple IPad the reported location for the internet showed Yatla - Yatla is a jail / prison in Adelaide - IPad and internet wireless modem previously registered under Jacqueline Pearce when showing this location - before VPN installation and security systems.

New Computer system has been registered in JC INNOVATIONS - New accounts and emails in JC INNOVATIONS, including security systems and passwords

- Microsoft account
- McAfee security
- Malwarebytes security
- Lastpass security
- GoDaddy email and domain hosting - Business premium - professional email and domain
- Gmail - personal account
- NordVPN security

New phone number - New sim card and account has been registered in a business account under JC INNOVATIONS, setup by Joshua Adams, Telstra, Kadina, Business Consultant - The personal phone account registered under Jacqueline Pearce had been closed and reported for fraudulent activity and red flagged for investigation.
The newly formed business account was red flagged to be watched for any suspicious activity and placed in restricted access, only to be accessed in store by Joshua Adams and the Manager Isabelle Oppeloar.

Security systems applied

- NordVPN
- Malwarebytes security
- McAfee Security
- Lastpass authenticator

Internet wireless modem - New sim card registered under JC INNOVATIONS

Apple IPad registered accounts and IPad registered under JC INNOVATIONS

- Goggle account
- Apple Playstore account

I have reported my business Visa card connected to my registered JC INNOVATIONS business bank account as lost and stolen, which is now closed and waiting for a new card since this reported notifications of suspicious activity in my new accounts.

I have changed the password of my Netflix account on the advise of the email notification and changed my Apple login to finger print login access and changed the password.

Previous activity of previous personal accounts - Phone and Toshiba laptop computer System recognised and documented over an 8 year period

- Unusual activity login reports - Computer system
- IP address conflictions
- Continuous Internet disruption and shut downs
- 135,000 malwares found on computer system
- Fraudulent emails from people impersonating a senators office containing information that I had not supplied and I had not supplied my email address
- Blocked emails / contact
- Blocked and altered phone text messages
- Excessive rise in billing
- Impersonating phone companies representatives and placing me on payment plans - Informed by the phone company OPTUS that the representative that addressed me and placed me on the payment plan was not a registered employee with their company
- Impersonating a representative / lawyer of a law firm - Gordon Legal, Melbourne when seeking legal advice and representation - representative name matched an electoral role department. Victoria and claimed that their firm does not represent victims of crime

My accounts have now been hacked for the second time, previously targeting my personal accounts and now targeting my new business accounts and systems registered in JC INNOVATIONS, not Jacqueline Pearce, which indicate specific targeting of the individual, Breeching all security systems and restricted access of phone account set up by Brennan, Pitstop Technologies, Kadina and Joshua Adams, Telstra Store, Kadina.

New business registered phone number and account of JC INNOVATIONS
Event: This number was given to my previous partner Vincent Bulone, Director of Research, Adelaide University, KTH, Sweden University before realised that my previous partner was involved in the targeting and connected to the other individuals involved in the targeting. Documented evidence supports his involvement. No reply. The next day after giving him this phone number I received a phone call from a representative of Energy Saver. I am not registered with any utility company as I live with my parents in Kadina. My new business registered phone number is registered as private / not on record for public access. I reported this phone call which I found suspicious as I had only registered the new number the day before to Brennan, Pitstop Technologies, Kadina. He informed me that their company receives similar calls from energy companies and that my number had been randomly picked and that I should not worry about it. I am still receiving these phone calls from this company.

Previously registered phone number - Registered under Jacqueline Pearce
Event : February 2020 - Escalated event, Telstra, Kadina - Blocked messages to Vincent Bulone while he was in Sweden, KTH Sweden University - Ph number: [redacted]
Telstra informed me that it was as if a switch had been turned off on the servers end in Sweden and they had reconnected the connection again.

Vincent Bulone has been identified in documented evidence after these events as being involved in the targeting and stolen business concepts from the privacy of my parents home in Kadina, hand written form, not installed on a computer or shared with a third party.

Individuals indentified in documented evidence - Targeting involving Intellectual property Theft and various forms of fraudulent activity and targeting - 27 years of targeting

- Microsoft
- Various government figures
- Michael Fetherstonhaugh
- Paul Gardner
- Peter Bannister
- Scott Bowman, Port Pirie Police Department
- Numerous members of the Port Pirie Police Department
- Motorcycle gangs - The Hells Angels - The Red Devils, Port Pirie - The Jokers
- Adelaide University
- Julia Gillard - University position - Connected to Vincent Bulone / previous partner

I am currently organising the documented evidence that I have collected over an 8 year period into file form and have informed Gordon Legal, Melbourne , Victoria via their website that I will be submitting the evidence and seeking their representation for conviction and prosecution against the individuals involved in the targeting as soon as the state boarders open and I am able to drive to Melbourne over the boarder. I am seeking as representation Peter Gordon, Gordon Legal, Melbourne, the law firms leading lawyer, who is involved in litigation with the Government involving the recent Robodebts created against Centrelink recipients, that also involved suicide to occur.

At this point until I press charges all individuals named above remain as alleged, in legal terms until court proceedings begin and they are charged with the targeted crimes which have occurred over a 27 year period - 1993 - 2020.

Targeting has occurred in every residential location , Wilimulka, Port Pirie, Adelaide and Kadina.

Requesting reports being made of Specific targeting of an individual and activity involved - Second hacking of now business accounts, not personal accounts after being newly created by your company as a registered client of Pitstop Technologies, Kadina :

- Telstra Store, Kadina - Joshua Adams - Manager, Isabelle Oppeloar
- Telstra head office - CEO
- McAfee security - CEO
- Malwarebytes security - CEO
- Samsung head office - CEO - second hacking of security systems installed on the purchased phone
- HP Computers - CEO - hacking of McAfee security system installed on the computer upon purchase
- Lastpass security - CEO
- GODaddy - CEO

Upon registering with GoDaddy, Business Premium I had informed them of the previous activity involving the hacking of my previous systems and that I had upgraded my system and security with your company. The representative informed me that if this activity occurred again that they were very willing to get involved and would use their higher authority to report this activity to the authorities of their country, America. This account is now compromised due to the second hacking of my accounts and devices and need to be informed and their authority to report this targeting executed.

I am requesting that all reports of this second Specific targeting of an individual be conducted via Skype services, as to report this activity to the CEO face to face of each company listed, as to identify the person that you are reporting this activity to as being the representative of that company. I am requesting that the Skype reports be recorded for legal purposes.

I am making this request as during the process of acquiring assistance and reporting this activity over an 8 year period, including the year 2020 I have encountered impersonating representatives of companies, including law firms, intercepted mail, blocked and altered text messages, fraudulent emails impersonating senators officers by using usual methods of phone calls, postal systems or email contact.

I am requesting that when the CEO's of these companies are contacted and this activity is reported that they are informed that the person involved, the victim, your registered client will not give a statement or reveal documented evidence in her possession to authorities until represented by a lawyer of Gordon Legal, Melbourne, Victoria - Peter Gordon.
This is a security measure as there are government figures and police officers involved.

I am requesting as a registered client of your company a Skype appointment being made in your office with Gordon Legal, Melbourne - Peter Gordon to report this activity and request Legal Assistance regarding this matter. I do not wish to seek any other representative of this law firm.

I thank you for your assistance concerning this matter.

Kind Regards
Jacqueline Pearce
Director: JC INNOVATIONS

CONTACT RECEIVED 25TH SEPTEMBER 2020

Gmail

Jacqueline Pearce [redacted]>

Ticket#646196/ Security Issues Has been updated

1 message

Pit Stop Technologies Business Support [redacted]>
To: [redacted]

30 September 2020 at 14:44

--REPLY above this line to respond--

Hi Jacqueline,

Having provided your documents to the manager I have been advised to contact you and outline the following.

Our technicians previously improved your security to the full extent of our ability. While conducting these works, our technicians did not find any remote access to your devices, or any other flags that indicate a hacking has occurred.

Beyond this, it is outside the scope of the work we can provide for us to be responsible for your mobile phone / PC any further. If you require us to send an email to your lawyer outlining the works we have performed on your devices, we can certainly do so if you provide us with their contact details.

While we understand your current situation, it appears there is no further work that we can do to assist you beyond outlining our previous work to your solicitor.

Thanks,

Mathew Brand

PITSTOP TECHNOLOGIES
KEEPING YOUR IT ON TRACK

98 Port Road | Kadina, SA 5554
Phone [redacted]

website

CONNECT[redacted] TO EMAIL ACCOUNT - holly.jackson@jinnovations.com.
THIS ACCOUNT HAS SUSPENDED DUE TO THE SUSPICIOUS ACTIVITY BY TWITTER - BLOCKED MARKETING OF PUBLISHED BOOK

Holly Jackson

From: Twitter <[redacted]>
Sent: Wednesday, 11 November 2020 10:08 AM - MARKETING OF PUBLISHE
To: Holly Jackson BOOK CONNECTED TO THI
Subject: Security alert: new or unusual Twitter login EMAIL - PUBLISHING HOU
CONTACT / CONTRACT

We noticed an attempt to log in to your account [redacted] that seems suspicious. Was this you?

If this was you

Just to be safe, to log in to this account you'll need to verify this is really you by entering the following single-use code.

[redacted]

If this wasn't you

Complete these steps now to protect your account.

- Change your password. You'll be logged out of all your active Twitter sessions except the one you're using at this time.
- Review the apps that have access to your account and revoke access to any unfamiliar apps. Learn more.

How do I know an email is from Twitter?

Links in this email will start with `https://` and contain `twitter.com`. Your browser will also display a padlock icon to let you know a site is secure.

Help Not my account Email security tips

This email was sent to @holly_jackson

Twitter, Inc. 1355 Market Street, Suite 900, San Francisco, CA 94103

TWITTER ACCOUNT - SUSPENDED