SCORE

FOR THE LIFE OF YOUR BUSINESS

Cybersecurity: Protecting Your Business from Hackers

For Startups or Continuing Businesses

By

Russell Seeney

Pacific Business Services, Inc.

Before We Start

Score.org

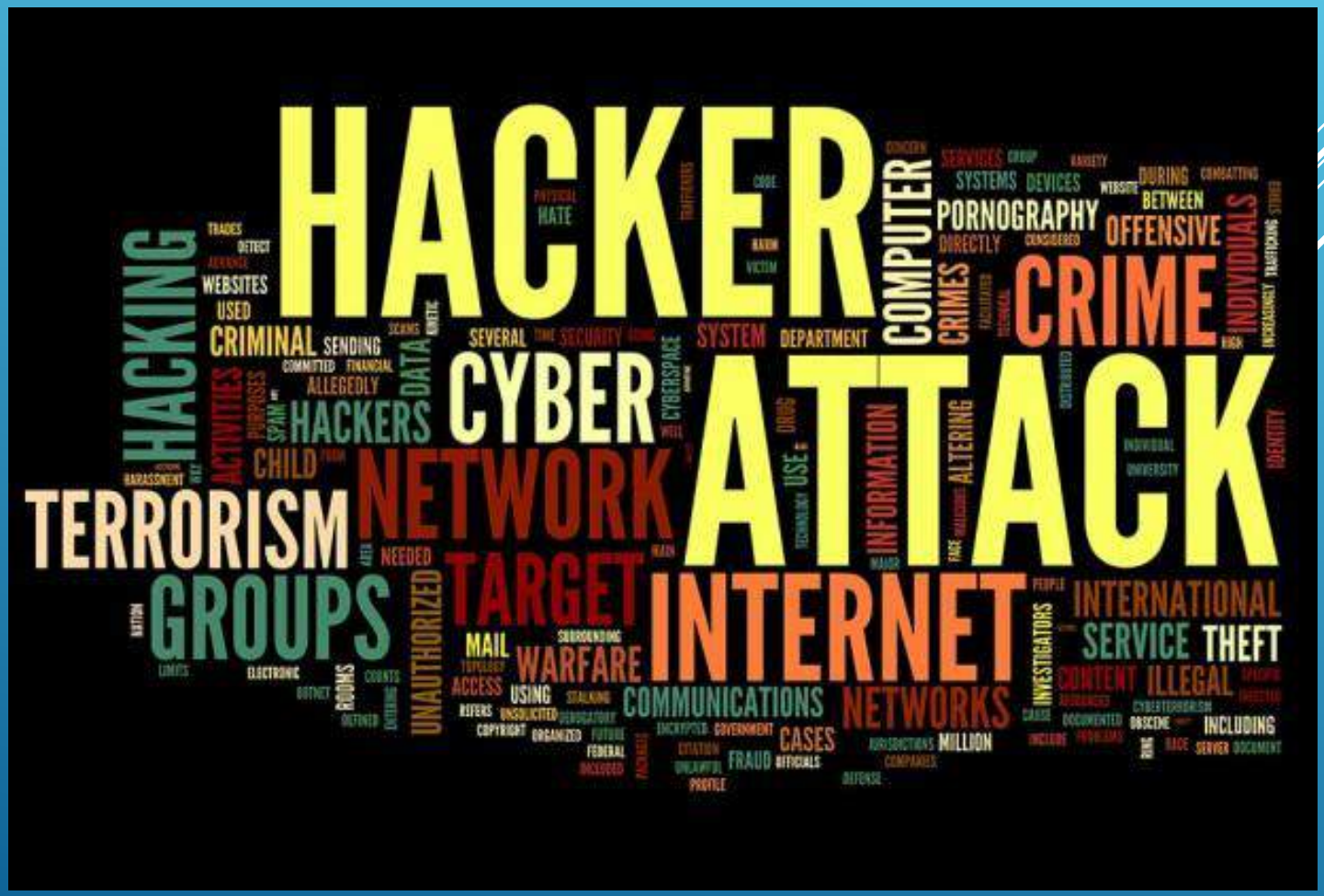
Score Hawaii

- Score is a National non-profit organization dedicated to providing educational and free mentoring services to entrepreneurs
- Score Hawaii is based in Honolulu and is a member chapter of the Score National organization
- If you are involved in starting or are already operating a business and would like a mentoring service, please go to Score.org webpage to register for free one-on-one mentoring service. Go to Score. Hawaii for webinar updates
- For those interested in volunteering, please visit Score.org webpage and register to be a Score volunteer

DISCLAIMER

- The information presented is for informational and educational purposes only.
- The opinions expressed during this presentation are the opinions of the presenter and no other.
- Contact your lawyer, banker, or other technology experts to obtain advice with respect to any issues or problems associated with technology security

Cybersecurity:
Protecting Your Business from Hackers



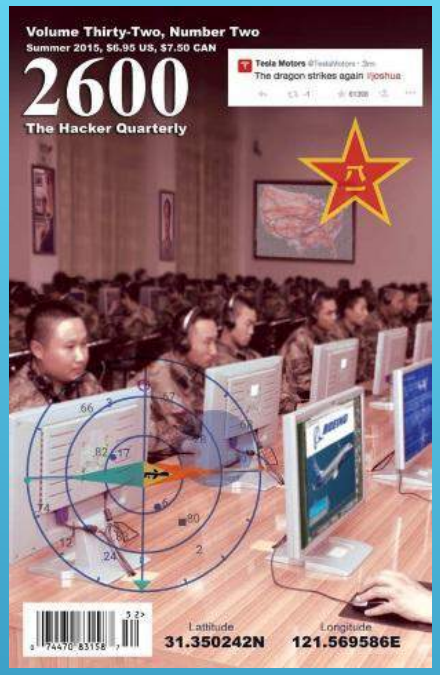
HACKER BACKGROUND

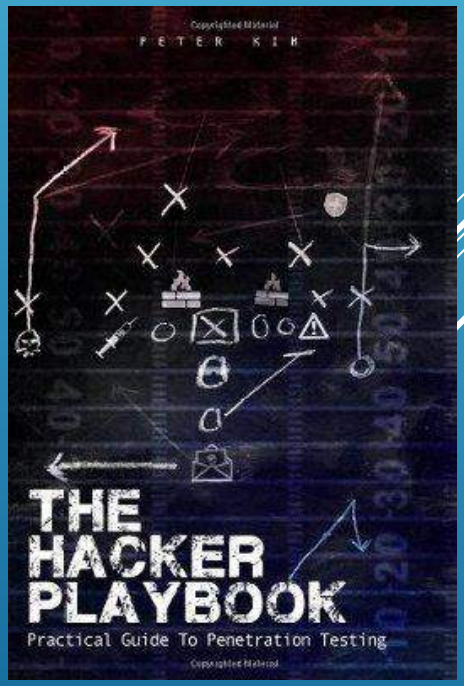
LINKS CAN'T BE THAT BAD !!

THE BAD GUYS

WHAT ARE THE ISSUES?

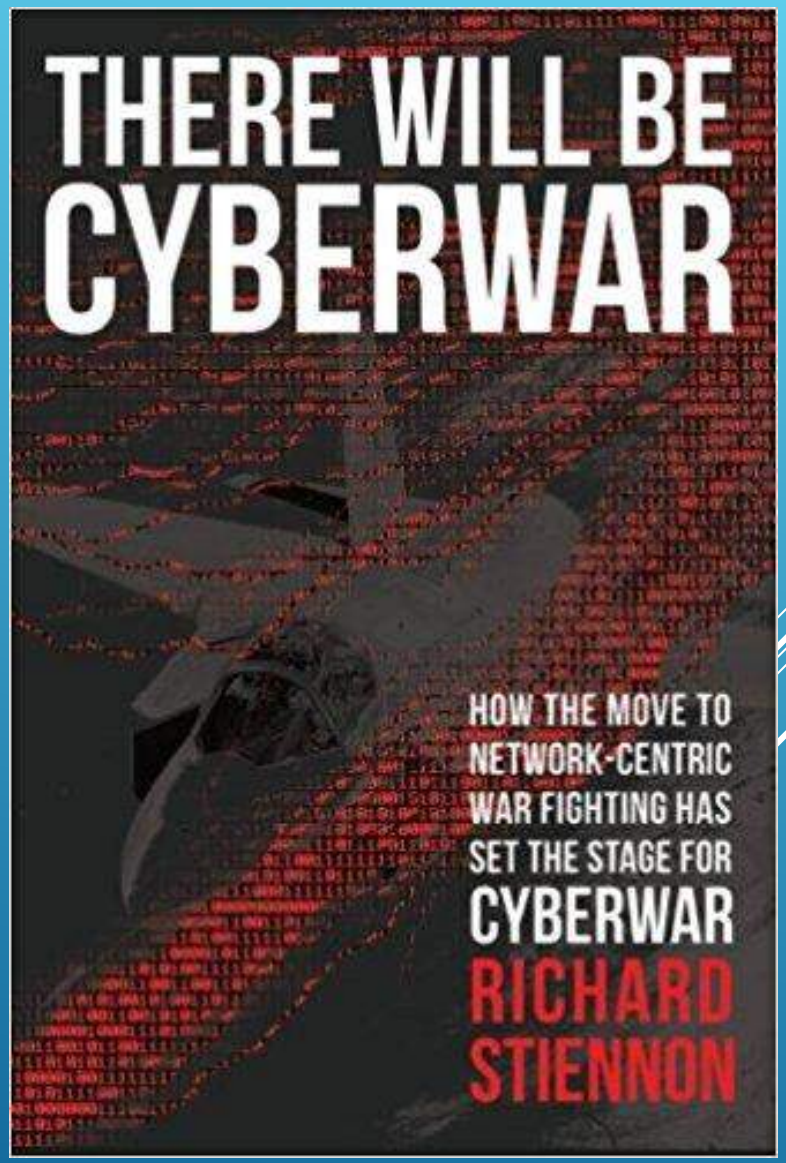
- **The hackers have handbooks**
- **The hackers are State Sponsored such as Russia, China, North Korea, Iran.**
- **The mobster gangs are real and they are hiring the state sponsored hackers.**
- **The hacktivists are a much smaller percentage and many are doing it for fun.**





WHAT ARE THEY LOOKING FOR?

- They are looking for names, social security numbers, passwords, addresses, credit card numbers.
- Their primary goal is to steal as many as possible and they are probably not going to be the ones to actually use this information.
- The approach is simple, you may think I don't have anything worth stealing. But it might be *who* you know.
- Most times, their goal is to resell the information.
- Medical records are currently being sold for $15 up to $250 per each record.



YOUR TECH WORLD IN CONTEXT, MOBILE, OFFICE LAN, WORK FROM HOME (WFH)

THE ATTACKER'S HAVE CHECKLISTS AND PROCESSES

- 1. Perform Reconnaissance (What is my IP)
- 2. Scanning and enumeration (you have ports like having a bunch of PO boxes)
- 3. Gaining access
- 4. Escalation of privileges
- 5. Maintaining access
- 6. Covering tracks and placing backdoors (go into hiding or stealth mode and wait)

Additional information: The cyber kill chain (CKC) is a classic cybersecurity model developed by the computer security incident response (CSIRT) team at Lockheed Martin.

PROTECT YOUR BUSINESS, YOUR WORK FROM HOME (WFH) SYSTEMS

PROTECTING YOURSELF

PERFORM A RISK ASSESSMENT

- List Assets such as PC, Server, Email (each evaluated separately)
- Value or score of importance of this asset (contains PII data, company data, customer data.
- Vulnerability such as unpatched system, power
- Threat against that vulnerability – virus, power outage
- Mitigation to protect against each threat
- Discussion about Cyber Insurance Add-on, and proof of mitigation steps taken

HOW TO PROTECT YOURSELF, YOUR COMPUTERS, YOUR NETWORK AND MOST IMPORTANTLY YOUR DATA

- Basic protection, create a backup to a Terabyte drive
- Make sure your firewall is turned on, go invisible
- Make sure your anti-virus is current and up to date.
- Install licensed software like MalwareBytes to complement your UPDATED anti-virus software.
- Make sure your Windows 10 updates are turned on and set to automatic.
- If you are still on Windows 7 Microsoft stopped generating security patches last year
- If you have programs like Office, Adobe, Java, etc make sure they are updated all the time.

MORE PREVENTION

- **Make your passwords complex, not 123456 or "Password" or p@$$w0rd**
- **Password cracking programs we use can crack this in a few seconds or a few minutes.**

- **L8t3r@lligat0r$2021! About 398 centuries to crack**
- **Make your password a phrase**
- **Don't use the same password everywhere. Once you decide on a password do something like ebay-mycoolpassword, paypal-mycoolpassword, facebook-mycoolpassword, fhb-mycoolpassword**
- **Force periodic password changes and yes that is a hassle**
- **Rename key accounts such as Administrator and Guest**

EXAMPLE TEST YOUR PASSWORD SITES

- Comparitech - Test your Password Strength
- https://www.comparitech.com/privacy-security-tools/password-strength-test/#password-generator-tool

- My1Login How secure is your password?
- https://www.my1login.com/resources/password-strength-test/

- Microsoft Password Strength Checker (Download and install)
- https://www.microsoft.com/store/productId/9WZDNCRDQRH5

EMAIL & IDENTITY LOSS PREVENTION
64% OF ATTACKS ARE BY USERS CLICKING A LINK.

- Email etiquette
- If you are sending a joke, an informational or discussion email to several or many people and you don't know what antivirus they have or how secure their computer is:
- Never ever send a bunch of names on the TO:, or CC: lines. Always always use the BCC: line.
- The reason is I might not be a bad guy but my computer might be infected and I have accidently downloaded an email sniffer and you have just given the bad guys a good valid list of your contacts in a few seconds.
- And to make it worse you may have given this to spammers and given the bad guys permission to spoof your friends.
- So never use the TO:, CC: lines and if you receive an email like that it is okay to reply (not reply all) the person to please never include your name this way.

BEFORE YOU ARE ATTACKED?

- As soon as possible, make a backup of your computer.
- Make a 2nd backup of important folders and data
- Get a TeraByte drive such as MyBook which has automatic backup software built-in
- Use it
- Check it periodically
- Make daily backups of the stuff you changed today (incremental)
- Use a program like Acronis to do the backup

TERABYTE BACKUP DISK DRIVES

Seagate Expansion Portable 4TB External Hard Drive Desktop HDD – USB 3.0 for PC Laptop (STEA4000400)

4.5 stars ~ 62,729

Personal Computers

$95.39 ~~$119.99~~

FREE Shipping by Amazon

In stock on December 31, 2020.

Western Digital – least reliable, cheapest and most popular
Seagate more reliable, inexpensive
Hitachi HGST – most reliable, cost a little more

BUT I HAVE AN APPLE MAC AND THEY CAN'T BE HACKED.

- Malware doesn't attempt to get into your machine without your knowledge - it is malicious software disguised as legitimate software. It tricks you into installing it as you would any other program, and then when it is installed it starts to gather information about you. In most instances it wants to get hold of your credit card or banking details and passes them on to nefarious individuals on the other end.

- Where things get tricky is that most Mac malware pretends to be the very thing you want to use to get rid of it. Most Mac malware seems to masquerade as antivirus or antimalware software. While there is no definitive list of OS X malware, here are some names to watch out for:
- ***MacDefender***
- ***MacProtector***
- ***MacSecurity***
- ***So, to be clear: these are the names of programs you should be avoiding on Apple computers.***

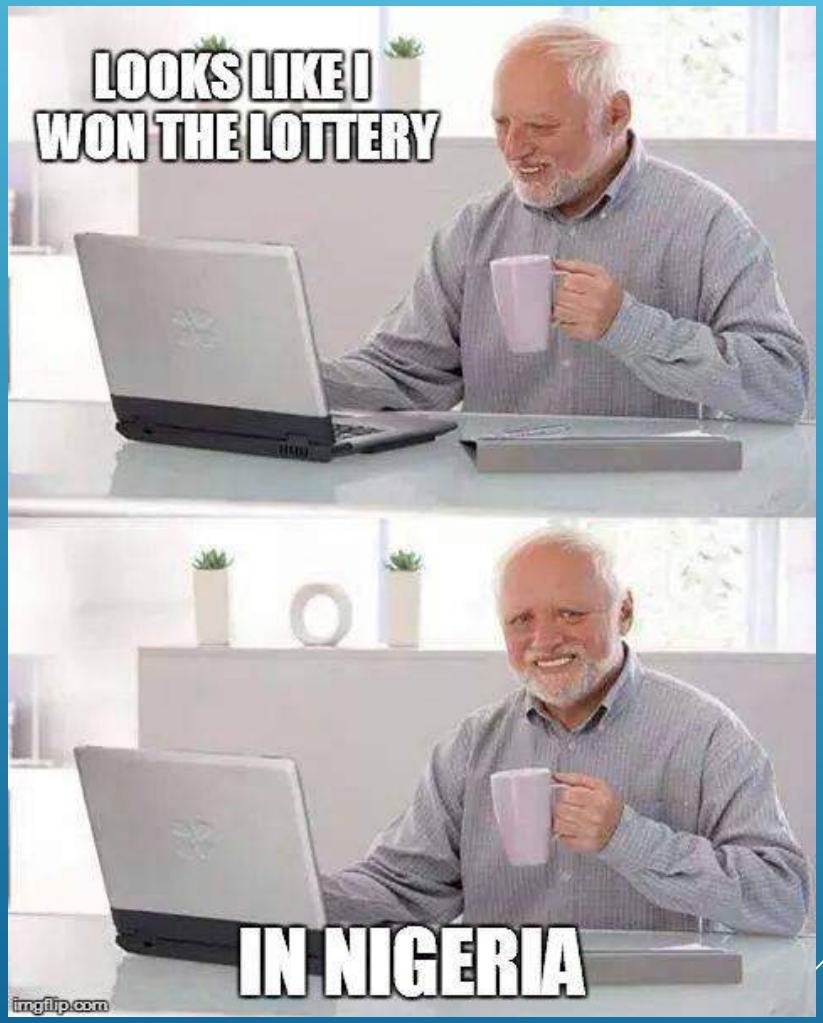
EVIDENCE

HOW DO I KNOW ?

WHAT TO WATCH FOR

- Misspellings and typos
- The www or http or URL is from somebody else, stop look and read before clicking.
- Incorrect information
- Generic names – Dear [NAME]
- Asking for user ID's, passwords, Social Security numbers, addresses, unlocking your account / click here schemes.
- ***Don't Click the pictures, attachment, download for more information, IF YOU DON'T KNOW WHO IT IS, DON'T CLICK IT !!***

I WON THE LOTTERY !

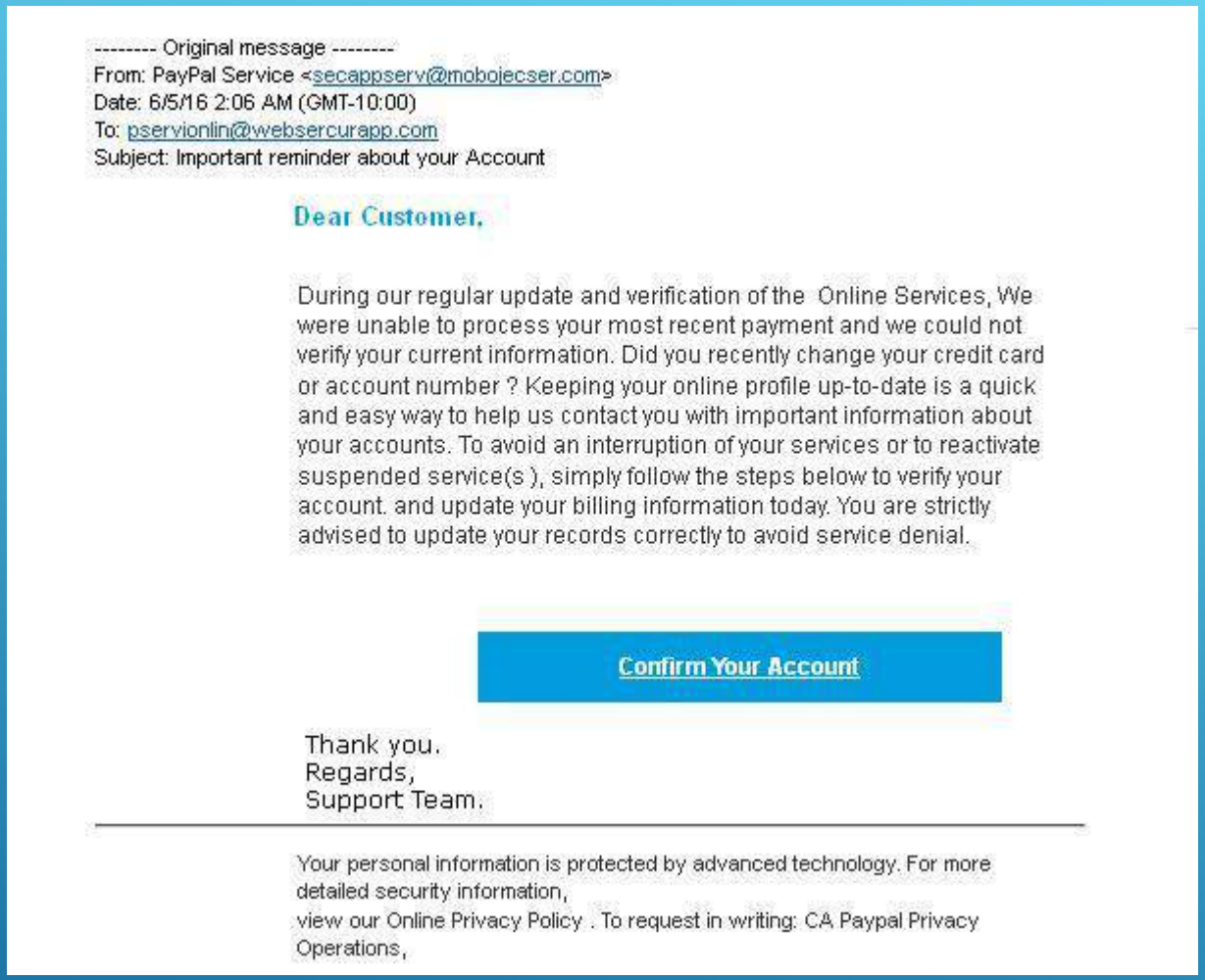


CAPITAL ONE BREACH

- Awareness trainings, especially with social engineering, spoof emails from trusted sources.
- The weakest link is an employee compromising the Network with spyware or Trojan Horse malware from nation state actor.
- The recent Capital One credit card hacking is an example. This hacking is an example for businesses to motivate themselves to beef up their security awareness training for internal staff and members / customers.

CAPITAL ONE BREACH

The hacker accessed the personal information of approximately 106 million card customers and applicants, **one** of the largest-ever data **breaches** of a **big** bank



-------- Original message --------
From: PayPal Service <secappserv@mobojecser.com>
Date: 6/5/16 2:06 AM (GMT-10:00)
To: pservionlin@webservcurapp.com
Subject: Important reminder about your Account

Dear Customer,

During our regular update and verification of the Online Services, We were unable to process your most recent payment and we could not verify your current information. Did you recently change your credit card or account number ? Keeping your online profile up-to-date is a quick and easy way to help us contact you with important information about your accounts. To avoid an interruption of your services or to reactivate suspended service(s), simply follow the steps below to verify your account. and update your billing information today. You are strictly advised to update your records correctly to avoid service denial.

Confirm Your Account

Thank you.
Regards,
Support Team.

Your personal information is protected by advanced technology. For more detailed security information,
view our Online Privacy Policy . To request in writing: CA Paypal Privacy Operations,

Sample bad guy phishing email from PayPal, eBay, Verizon, FBI, etc

Most common and most deadly

-------- Original message --------
From: PayPal Service <secappserv@mobojecser.com>
Date: 6/5/16 2:06 AM (GMT-10:00)
To: pservionlin@webservcurapp.com
Subject: Important reminder about your Account

Think like CSI / FBI, be suspicious
DO NOT CLICK, just delete

digitalyogionline.com/wp-content/themes/us/paypal/help/custom/resolveapp/verification/

PHISHING ATTACKS (MAN IN THE MIDDLE FAKE PAGE)

Entering your Access #, User ID, Password.

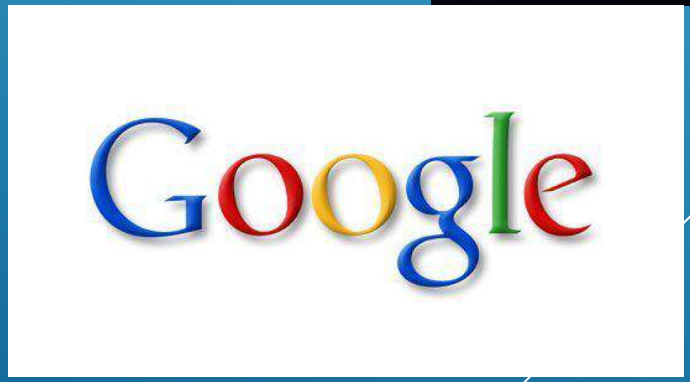
GOTCHA

Bad guys scrape what you typed keep a copy and then send a copy to the real web site.

Check the HTTP URL. Not real site.

Thank You.

SOCIAL MEDIA

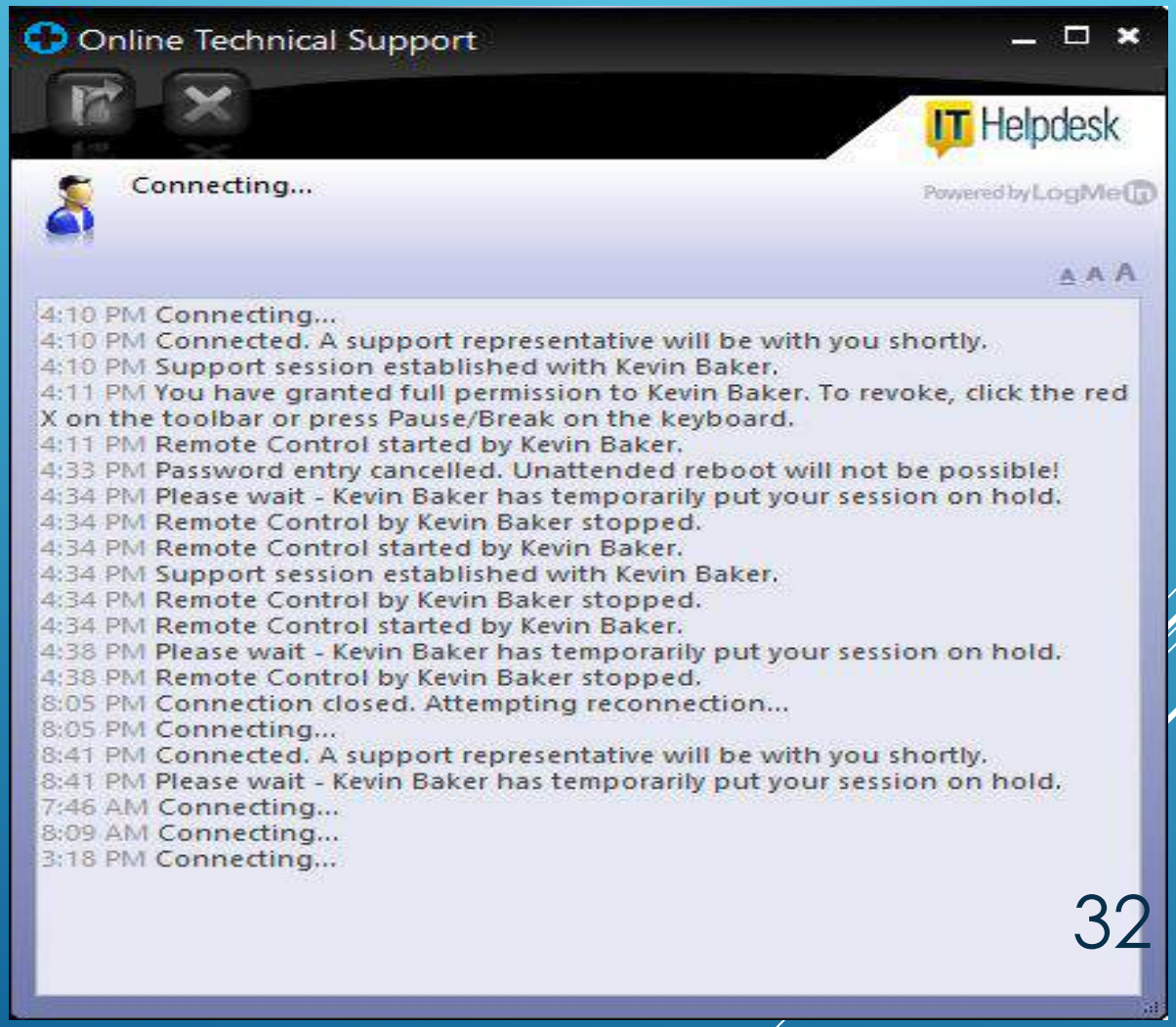


CALL FROM MICROSOFT TECHNICAL SUPPORT (IT IS NOT MICROSOFT !!)

- **Called from an Indian (other country) accented person claiming they are from Microsoft Windows Service Centre, he says that my computer has been hacked and they want my details to "fix the issues". They just need for you to do a simple check and they will have you back up and running clean.**
- **Microsoft will never call you like this and ask you to get access in to your computer.**
- **If you give them the keys (access) to the front door, your computer is now theirs, thank you very much.**

LIVE SAMPLE FROM ITHELPDESK SUPPORT

Actual sample from May 2017



STAY VIGILANT AGAINST BOGUS IRS, COVID-19 VACCINE CURES, UNEMPLOYMENT, STIMULUS, RED CROSS DISASTERS TELEPHONE CALLS AND EMAILS

- **IRS Tax Tip 2015-20, February 17, 2015**
- Tax scams take many different forms. Recently, the most common scams are phone calls and emails from thieves who pretend to be from the IRS. They use the IRS name, logo or a fake website to try to steal your money. They may try to steal your identity too. Here are several tips from the IRS to help you avoid being a victim of these tax scams:

- ***The real IRS will not*:**
- Initiate contact with you by phone, email, text or social media to ask for your personal or financial information.
- Call you and demand immediate payment. The IRS will not call about taxes you owe without first mailing you a bill.
- Require that you pay your taxes a certain way. For example, telling you to pay with a prepaid debit card.
- Be wary if you get a phone call from someone who claims to be from the IRS and demands that you pay immediately.

NEVER EVER CLICK ON ATTACHMENTS THAT CAN ENCRYPT YOUR FILES. IF IT LOOKS TOO GOOD TO BE TRUE, IT IS. THIS RANSOMWARE IS DEADLY AND ALMOST ALWAYS THE COMPUTER NEEDS TO BE RESTORED FROM ONE OF YOUR BACKUPS-PERIOD. IT IS BAD.


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy

WANNACRYPT - STARTED FRIDAY MORNING. MAY12TH, 2017.

- **Was in 40 Countries by evening**
- **Was in 90 Countries by Saturday morning**
- **Was in 150 countries by Monday morning**
- **Kill Switch was found on Sunday, May 14th, but it took time to slow the spread of the ransomware**
- **Warnings about that it should be done, don't click anything, stay vigilant, there could be mutations being developed.**

FREE WIFI CAN BE EXPENSIVE

- **FREE – Read the WiFi disclaimers at airports, StarBucks, Ala Moana, Kahala, TWCID, on an airplane, etc, etc all say it is your responsibility to protect yourself.**
- **Make sure your firewall is on and set for PUBLIC not private network.**
- **Make sure Antivirus is on and updated and running**
- **Watch and be suspicious of the people using the Internet around you, watch for unexpected popups**

INCIDENT RESPONSE

Federal Bureau of Investigation (FBI)

Internet Crime Complaint Center (IC3)

https://www.ic3.gov/

InfraGard.org

iLEEP offering services to non-LEO users.

Malware Investigator to submit actual Malware samples.

DHS CISA CERT reporting

Sample incident response phases are:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

INCIDENT RESPONSE (CONT)

- **Google CISRP or NIST CISRP**
- Cybersecurity Incident Response Plan {CSIRP Checklist 2021}

- NIST - National Institute of Standards and Technology
- SP 800-61 Rev. 2 (2012)
- Computer Security Incident Handling Guide

- Recovery Time Objective (RTO) and
- Recovery Point Objective (RPO)
- Keep an INCIDENT LOG, date, time, action, person, department, computer or function or application

WHAT WE LEARNED

YOU ARE IN CHARGE OF PROTECTING YOUR DESKTOPS, YOUR NETWORK, YOUR DATA. THE BAD GUYS ARE PLAYING FOR KEEPS, YOU NEED TO ALSO.

WHO DO YOU WANT PROTECTING YOUR COMPUTER?

THANK YOU

QUESTIONS?

Email: RSeeney@PBSHawaii.com
Pacific Business Services, Inc.
Tel: 808-545-3722
or hawaii.score.org Hawaii | SCORE