HCS New Zealand Ltd

Client Resources Publication

Network Security in the Workplace

More supporting information can be found on our website and blog at

www.pcheroes.co.nz

Keep Safe in the Digital Wild West

Awareness and Best Practices are the Best Line of Defense

The internet – for all of its growth and progress – has unfortunately become more insecure and dangerous than ever in the 21st century. With all the security investment, and anti-hacking organizations, the number of incidents and the cost to Western Civilization is still skyrocketing.

In an attempt to minimize security incidents on Client networks – we hope that this document will raise Awareness of how people may try to intrude, and more importantly how all members of an organization can take practicable steps to keep themselves safe while conducting their operations online.

Antivirus, Anti-Malware and Immunization – The Last Line of Defense

Everyone needs an Antivirus – HOWEVER – this is literally the front door of your network. If an intrusion is being blocked by your Antivirus, then it potentially has already made it too far.

Additionally, to your Antivirus (which is a real-time layer) you need a secondary tool to run a "Once off Scan" for other items such as Malware, Adware and other Potentially Unwanted Programs (PUPs).

We recommend;

- **Antivirus:** A paid antivirus such as ESET Nod32 Antivirus (http://www.eset.co.nz/).
- **AND:** An Ad-Block extension for your Browsers (https://chrome.google.com/webstore/detail/adblock/)
- **AND:** A free Anti Malware application such as Malware bytes (http://www.malwarebytes.org/).
- **AND:** Lastly an Immunization with SpyBot SD (www.safer-networking.org).

Please note that these recommendations change constantly as the security industry, and/or the effectiveness of the above products change.

Warning – Do not run multiple specific "Anti-Virus" software otherwise they can render each other ineffective. One must be clearly marked as an Anti-malware or Second Opinion Scanner.

Backup, Backup, Backup! – Your Only Failsafe

This is the only way to quickly recover business operations after an incident that results in data loss of any operational or support data.

It is CRITICAL that all important business and operational data is backed up in multiple places.

We recommend the following;

1. On-Site Backup on an automated basis.
2. Cloud Based or Off Site Backup on an Automated (or procedural) basis.

Important - Both of the above backup solutions should ideally use some form of 'File Versioning' to provide some protection against crypto viruses.

We use a combination of On-Site backups – for fast recoveries, and cloud based Backups – which are used in DRP situations where On-Site backups are not available (i.e. due to Fire, Theft or Otherwise).

Please contact us if you need support with cost effective Cloud and On-Site backup solutions.

Keep Critical Software up to Date

Often updates are Security Patches released specifically to address a potential hole or security issue in your critical software systems (including Windows, MacOS, Office, and other applications).

Although updates can sometimes open the door to other potential glitches (if those developers release patches that have not been properly tested) – however juxtaposed to this it does ensure that the software applications at least are patched to all known threats – and therefore the risks of Security incidents arising from that mode of attack is effectively minimized.

Auto-fill and Auto-save within your Browsers

We do not recommend using Auto-Fill or Auto-Save for Passwords or Credit Cards in your browser.

You will see this as "Do you want Chrome to remember your password for this site?" or something similar. Click "Never" or if this is not an option just click "No".

Better yet – check our blog for instructions on how to stop Auto Fill from trying to remember your passwords.

Protect your Accounts with Strong Passwords and Two Factor Authentication

Although it may seem like there is not much damage a cracker can do by getting into your random accounts – in fact the cracker will utilize this account access to gather as much intelligence on you, and your contacts, as possible.

This information makes social engineering attacks much easier – as they can often bypass your basic instincts simply by quoting a few of your trusted contacts names. They will equally use this information to potentially target any of your contacts they may be aware of as well.

For this reason, it is best to keep crackers out of ANY accounts you own;

- Choose strong passwords and do not disclose these to anyone.
- Use a Paid Password manager such as Last Pass (http://lastpass.com/) to manage these passwords across devices.
- Enable Two Factor Authentication (TFA) where ever possible – such as on Banking Transactions, when logging into Email from a New PC, etc. Just ask your provider for more information on Two Factor Authentication – as most services will provide these options to combat password breaches.

Other Means of Minimizing Harm (Employed Internally by Technical Staff)

- Vigilance in systems setup – i.e. Not leaving redundant ports open, etc.
- Hardware based defenses – i.e. Hardware firewalls, and Antiviruses – which can effectively either block a virus in the first place, or at least stop the virus from "phoning home" and executing the stage 2 infection.
- Limit access to information – if people don't need access to it, then don't grant it.
- Network Segmentation – dividing up of Corporate Networks to create multiple perimeter defenses across a company group to isolate any potential risks.
- Document potential threats – actually document the potential threats to a network – this enabling you to mitigate the risks posed rather than leaving them unknown.

Trickery used by 'Crackers'

And simple rules to help Detect and Catch these tricks.

The vast majority of security breaches (big and small) in corporate environments has employed some form of trickery in order to dupe someone (usually a staff member) into infecting a single PC (or Point of Entry).

Malicious Advertising

These appear all over the internet and are most often targeting credible and highly exposed websites. Most recently we have found adverts leading people to infected sites on Facebook.

Use Ad Blockers where ever possible (https://chrome.google.com/webstore/detail/adblock/) – and **simply ignore most (if not all) advertising on the internet**.

If an advert piques your attention –

Use Google as a source to look for "new" or "interesting" topics – because they are constantly testing websites and will not allow websites trying to infect people into their listings.

Otherwise the malicious adverts you may see usually take the following forms;

- Highly interesting, unlikely, or unrealistic articles. If it piques your interest, search it on Google to confirm.
- Or such as "You are infected with X viruses, Click Here to remove" or "Your PC is running too slow. Click here to Speed it up".

Emails, Messages and Social Network posts - from both Friends and Strangers

This is by far the most widely used distribution network for Viruses, Trojans and various forms of malware and deviant people on the internet. If this malware has infected one of your contacts – then it MAY be posing as that person to infect you. Or in more specific, or targeted cases, a human being themselves may approach you via these mediums.

This is called a Social Engineering attack – whereby they establish trust via your contacts or information they may know in order to manipulate a target into performing some action. Most commonly a link in the form of a Phishing Attack, or Infected Website.

See below for further information on these types of attacks

Simple Rule: Confirm all file transfers and links received verbally with the sender – unless it was something you had specifically requested or was expecting.

Phone Calls

We have heard of people posing to be from the following agencies – and typically they will already have and quote credible information on you to convince you it's a real call;

- Microsoft, Apple, or Otherwise
- IRD
- Banks
- Spark
- Or virtually any organization which they can somehow link you personally to.

Simple Rule: for ANY AND ALL COLD CALLS requiring you to furbish information or confirm any details –

1. Do not disclose nor confirm any information to the caller.
2. Ask the caller where they work and which division they are from.
3. Tell them that you would like to ring them back on their listed number before disclosing any information.
4. They will more than likely try to provide you with this a number to ring back on **– DO NOT RING THE NUMBER PROVIDED BY THE COLD CALLER.** Rather proceed to look up the provider on Google and use their OFFICIAL website to provide you with the correct phone numbers to ring.
5. Immediately ask for the Person at the Division that called and proceed to discuss if they exist.
6. If they do not exist – advise the provider that you have just been contacted by someone posing to be from their organization. And well done – your vigilance has just obverted a potentially major life altering event!

If you have identified them as a scam – simply tell them that your aware of the scam and hang up. They will certainly act seriously offended by your implication, and will attempt to convince you otherwise. Simply hang up after alerting them, and do not give them a chance to speak any further.

Do not attempt to play with them - these people have real ties with real criminal syndicates and you do not want to encourage 'more' targeted attacks.

If you believe you have been scammed already;

1. Immediately change any affected passwords through a CLEAN (un-affected) device.
2. Bring your affected devices into an ICT professional for investigation and disinfection.

Phishing Scams

This is when someone sends you an email, or message of some form – posing to be representing a reputable organization. Most commonly you see this as bank or provider asking you to verify your username, password or other compromising details about your account.

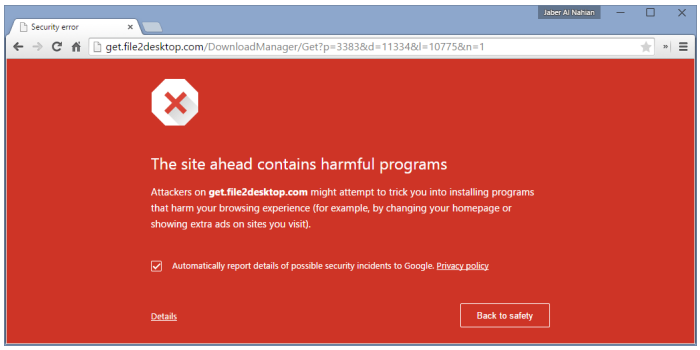
Almost all of these link to a page which looks absolutely correct – but which has been designed as a "replica" in order to skim your information once entered into the site.

This is an example of how a "phishing scam" can look.

Simple Rule: unless you were expecting them - simply never trust links that have been sent to you via email, messenger or otherwise. Always use your own bookmarks or navigate to the website via the URL or Google.

Reputable and Ill-Reputable Websites

Aside from the obvious websites of ill-repute – some reputable websites can be infected by a virus or may have an intruder on their servers who leaves behind all sorts of treasures to infect unsuspecting customers.



If you receive a warning when trying to access a reputable website, avoid that website until their admin staff have resolved the issue.

Simple Rule: ensure you always have a working and up to date antivirus installed. Use ad blockers (as covered above) and avoid websites that may be ill-reputable in nature.

Deep Web

There has been a lot of reference to the 'deep web' or the 'dark web' lately in the media.

This is a segment of the web which not accessible from the mainstream internet and can only be accessed using special tools – however is >90% dominated and run by criminal elements of the internet.

Simple Rule: It is strongly recommended that no one for any reason should go digging around the "deep web".

Seemingly random USB's or DVD's.

If you find a DVD, CD or USB sitting in ANY public location – especially your company's car park – destroy it.

DO NOT insert this into ANY work, or personal PC. Please report any instances of this on your company premises immediately to your IT Department – as it could mean you may be the subject to a targeted attack and it must be prevented (or halted if already underway from another form of trickery).

Simple Rule: Do not use any USB or media which you are not sure of the content.

Public Wi-Fi

Much information can be captured in broadcasting account login details, or otherwise, through a widely accessed network. This is called a "Man in the Middle" attack.

There are scripts which allow people to poison networks relatively quickly – who can then begin intercepting, recording and/or manipulating information through that network. It is best to ONLY use your own Wi-Fi networks – such as off a Cellphone, Home or Work.

Simple Rule: Do not use publicly or widely accessible networks such as internet cafes, free or paid WIFI, and student networks to access sensitive information or accounts.

Most mediums of communication are NOT private

Most electronic methods of communication methods these days should be considered NOT private. Whether they are being listened to by Government organizations for the purpose of National Security, Massive IT providers such as Apple or Google for the purpose of Commercial development, or Script Kiddies, and otherwise for the purpose of theft and malicious activity.

Simple Rule: You should never broadcast over any electronic network any information which is considered sensitive or could be used against you or others to inflict harm.

