PROFiT
Prevention of Fraud in Travel

THE COUNTER FRAUD CAMPAIGN 2019

PART 18: OTHER WAYS DATA IS LOST

Prevention of Fraud in Travel (PROFiT) and the Fraud Intelligence Network (FIN) are working with the City of London Police to reduce fraud in the travel industry. PART 18 looks at some of the ways you may be unaware of that your data can be compromised and identifies how to reduce the risk.

PROFiT is the only official travel industry counter fraud body. We work on your behalf to carry out analysis and research, disseminate best practice and disrupt crime.

Find out how you can join the fight against crime. Contact via: contactus@profit.uk.com

If your website is subjected to cybercrime including using one of the methods outlined in this email campaign, then report it to **ACTION FRAUD**.
USE THE ONLINE REPORTING TOOL: https://reporting.actionfraud.police.uk/login
OR CALL ACTION FRAUD: 0300 123 2040 **(**helpline 24/7 for live attacks 8am till 8pm for others**)**

OTHER WAYS DATA CAN BE LOST

1.0 In the past few editions of the email campaign we have identified some of the ways people that might want to steal your data can do so and give you the reasons why they do it. We have also identified your main vulnerabilities and presented some ideas on how these can be countered.

1.2 In this edition we look at some of the less obvious ways your data may be compromised. Some of these methods are so simple you may not consider them as a vulnerability even if data does become compromised. We do not wish to give you sleepless nights and so we continue to identify some simple ways that you can reduce the risks.

UNAUTHORISED DATA DOWNLOADING

2.0 USB[1] sticks, flash drives, memory sticks, or pen drives; whatever you want to call them, these are devices that plug into a port on your computer and allow files, data, or documents to be copied and removed by staff, or 3rd parties that discover your password, or those that find the computer left open and accessible.

2.1 This method of data loss is sometimes used by criminals who bribe low paid staff in call centres (especially overseas call centres) or those working as home-workers, in order to steal identities. The passengers personal and bank details end up on the 'dark web' being used to commit fraud, people trafficking and similar crimes.

AVOIDING UNAUTHORISED DATA DOWNLOADING

2.2 The best way to ensure that your business is not the victim of a data download is to secure the ports on all computers and laptops when they are used in unsecured locations or where staff are not required to use the ports. There are a few ways of securing ports to prevent them being misused. The most extreme method of securing ports is to disconnect them. However, most of us do not want to go that far so here are a few more methods.

[1] USB = Universal Serial Bus

2.3 Microsoft has a built-in capability to lock ports which is free and easy to implement but as it changes the registry it is an uncompromising solution. The methodology for this approach can be found here: https://support.microsoft.com/en-us/help/823732/how-can-i-prevent-users-from-connecting-to-a-usb-storage-device.

2.4 USB port locks (also known as Kensington port locks) are commercially available which plug into the device ports and lock in place thus allowing a port to be secured and unsecured as necessary in the future. These are mechanical devices which are easy to fit. There is also various software available to purchase which offers flexibility. Many can assign read only access, read/write ability, complete denial or full control to certain devices or files. The software can be programmed to allow only certain media, like a keyboard or mouse, but can deny everything else. Temporary or scheduled access can be given to certain media or file types, and control over which applications users are permitted to transfer to and from removable devices.

ACCIDENTAL DATA LOSS

3.0 There are obvious ways that data can be accidentally lost. If a laptop or moveable media is lost or stolen and the device has not been password protected or data encrypted, then it is vulnerable, and this is a common occurrence.

3.1 Another less obvious way that data can be lost is for a file being sent to the wrong email address. Due to email address autofill miss-directing email is easy to do and why every business email should include a message saying that the contents are for the intended recipient only and give instructions on what to do in case they are sent to the wrong person.

3.2 Don't forget your 3rd party consultants! When a company employs a 3rd party to carry out a specific function or advise the board these 3rd parties are often given remote access through a VPN[2] or Citrix channel. Your systems are secure; the gateway into your systems is secure; the VPN or Citrix channel is secure; but what about the laptop that is connecting to them owned by the 3rd party? On more than one occasion we have found systems compromised because the 3rd party consultant has already been compromised, or inadequate security. Worse still careless consultants have been known to keep the passwords and login for each of their clients in the unsecured address book.

AVOIDING PROBLEMS WITH ACCIDENTAL DATA LOSS

3.3 Any file that holds important information should never be sent by email. If you really must send the data put it on a form of moveable media that can be encrypted, and password protected and make sure the password is strong. Send it by signed for courier service.

3.4 All devices that are taken out of the office should have a strong password that is changed periodically and at least 2 stage authentications before anyone can gain access to the contents. Where important systems and data access is required to be used out of the office the files and data should be encrypted with strong encryption and password protected. A privacy filter should also be considered. 3rd parties that are trusted enough to be given system access should be able to prove that their security meets your requirements, and this can form part of the contractual terms.

KEYLOGGERS

4.0 A keylogger (**key**stroke **logger**) is a program that records all of the keystrokes on a computer. Keyloggers are used by criminals and rogue staff to steal data, identify passwords, and steal account details to commit fraud. In the early days a keylogger would be a form of malware injected onto a computer via a phishing spam email. The most commonly encountered keyloggers identified in the travel industry nowadays are in the form of an unauthorised USB stick placed into a spare port on computer.

4.1 Keyloggers are often found being used at less supervised sites away from head office such as in shops, at homeworkers premises and call centres (often overseas). This is especially true of areas

[2] Virtual Personal Network

where security and vigilance may be lowered.

AVOIDING PROBLEMS WITH KEYLOGGERS

4.2 In order to prevent external keylogger drives being used you can disable all ports on equipment used in areas where the risk is higher (as explained above in the section on unauthorised data downloads). The best way to protect yourself from keylogger programs is to install anti-virus or security software that warns you when any new programs are being installed. You should also make sure no unauthorized people have access to your computers. Carry out regular unannounced checks on all devices that do have active ports to ensure that keyloggers are not being used.

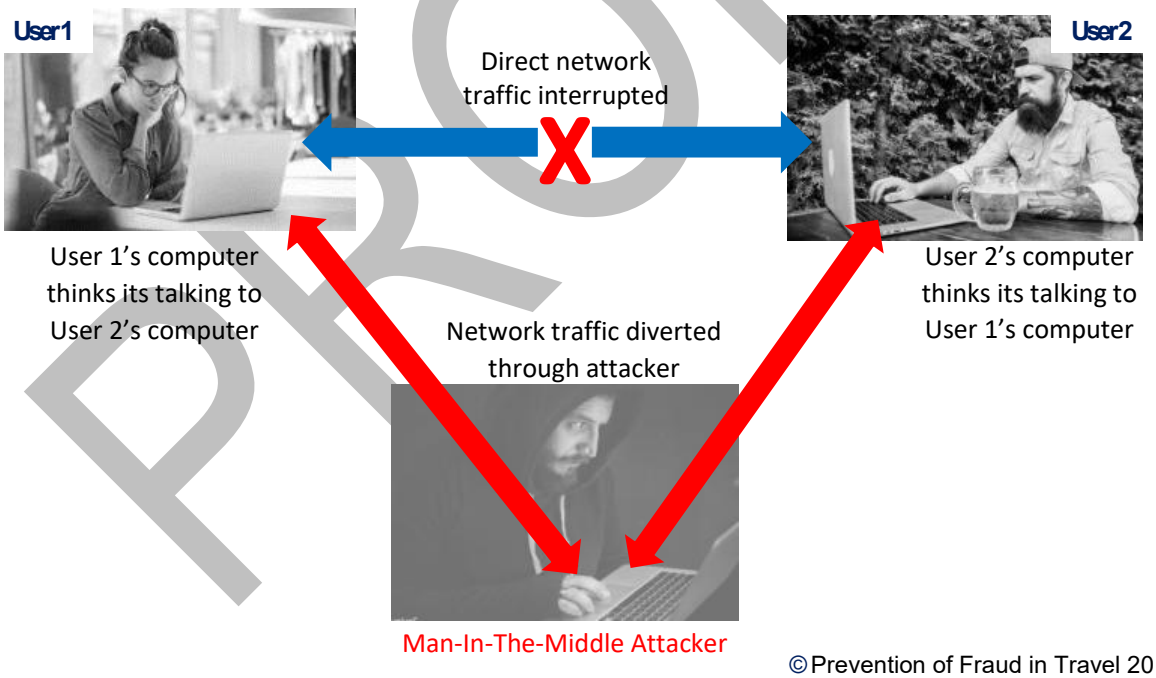
MAN-IN-THE-MIDDLE ATTACKS (MITM)

MITM ATTACKS IN PUBLIC SPACES

4.0 It's a common sight; you pop into your local coffee shop and there are several people working on their laptops or reading emails. This benign scene belies the dangers that exist in undertaking this seemingly innocent and praiseworthy activity. Public spaces such as coffee shops, hotel lobbies and trains are all areas where you could become the victim of a MITM attack.

4.1 A MITM attack occurs when you send data across the internet and an unauthorised third person in between you and the recipient intercepts it. If you have employees that like to work in public spaces, then you should be aware that these are common places that the best known form of MITM attacks take place using a device called a 'packet sniffer' and in this case a Wi-Fi Pineapple, but what is less well known is that these types of attack can occur anywhere.

A TYPICAL MAN-IN-THE-MIDDLE ATTACK



4.2 With this type of attack the malicious actor is subverting legitimate and readily available equipment designed to carry out penetration testing in order to commit crime. By sitting in between your connection and your recipient, the attacker can view all of the data that you intend to send over the internet. This can be especially dangerous if you intend to do online shopping, user personal data, or do online banking.

4.3 If the website isn't using HTTPS[3] (the secured version of the HTTP protocol) then your data is unencrypted and fully viewable to the attacker; but even if the site *is* using HTTPS, the attacker could spoof the real website, offering you a fake copy in order to collect your data. In this case when you are in the coffee shop you would apparently see the coffee shop Wi-Fi and when you use their code to gain access it will divert through the attackers false copy and WiFi Pineapple and connect to the genuine site as usual. You will be none the wiser.

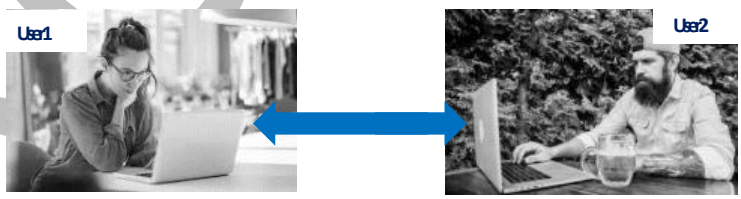
4.4 There are various types of MITM attacks.

- **Rogue access points** are set up to trick computers that automatically connect to Wi-Fi by posing as legitimate public networks. These rogue networks often monitor traffic and steal sensitive information.
- **Address resolution spoofing** involves a malicious node on a local area network posing as another machine to trick a victim into connecting to it before passing traffic on to the legitimate node.
- **mDNS spoofing** fools network devices into connecting to fake addresses. mDNS is used to match names to addresses on local area networks, and when spoofed give malicious machines access to vulnerable computers and IoT hardware.
- **DNS spoofing** is commonly used to trick internet users into connecting to fake websites set up to look like real ones. This method is common in online banking fraud and other account hijacking attacks.

The legitimate user will be unaware that anything untoward has occurred.

MITM ATTACKS IN SECURED PLACES

4.5 There are several weaknesses with the way that the internet works; for example, an attacker can access data on an HTTPS secured website by using a tool like [4]SSLStrip to remove the HTTPS encryption. Many people have an over simplistic way that the internet works. The average internet user, when asked to draw a map of their connection to a website, will typically show it going straight from point A to point B (their computer directly to the other user or website). Some people might include a point for their modem/router or their ISP[5], but beyond that it's generally a very simple diagram. The truth is that it is a complicated map and it will have multiple places where a MITM attack can take place.



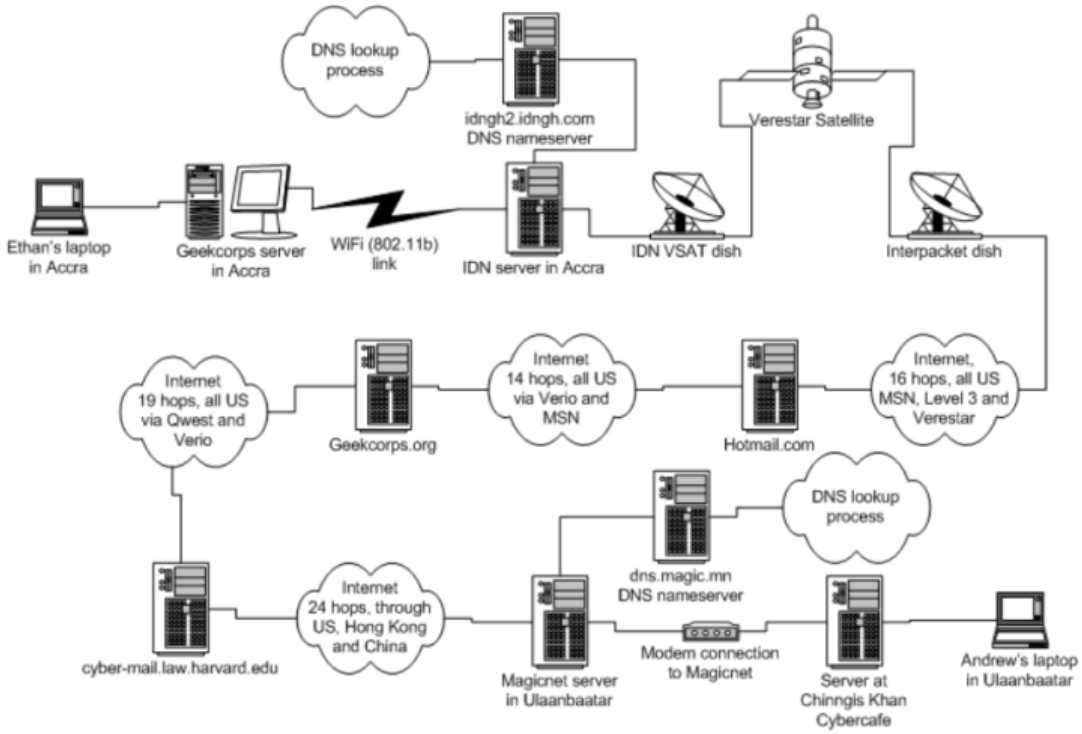
Users think that their internet connection is directly with the other party

4.6 Every operating system has a built-in function called "traceroute" or some variation upon it. This tool can be accessed on Windows simply by opening the command prompt and typing: tracert thesslstore.com. Doing this will show you part of the route your connection travelled on the way to its destination – up to 30 hops or gateways. Each one of those IP addresses is a device that your connection is being routed through. If you repeat the traceroute command, you may find it shows a different path being taken by your message.

4.7 When you enter a URL[6] into your address bar your browser sends a DNS[7] request. DNS are like the internet's phone book. They show your browser the IP address associated with the given URL and help find the quickest path there. Your communication is handed from device-to-device until it reaches its destination. As part of the Digital Democracy program Harvard University published a module entitled an 'Introduction to Internet Architecture and Institutes' which featured an email

[3] HTTPS = Hypertext Transfer Protocol Secure
[4] SSL = Secure Socket Layer
[5] ISP = Internet Service Provider
[6] URL = Uniform Resource Locator
[7] DNS = Domain Name Servers

conversation between a Research Assistant in Mongolia and a Scientist in Ghana. The communication route was as follows:



Harvard University illustration of an email between a Scientists computer in Ghana and a research student in Mongolia

4.8 Ethan and Andrew's conversations are routed through over 70 hops. Most of the gateways in transit are not secure which is typical of the internet infrastructure. Not only does this permit malicious MITM attacks to occur through these unsecured devices, but this is also how botnets can be created. Unsecured devices on the internet can be identified by criminals using a search engine type called a Sentient Hyper-Optimised Data Access Network SHODAN[8]. SHODAN scans the internet and returns full information on any unsecured device out there.

4.9 SHODAN gives criminals the ability to track down specific devices and look for high value MITM targets, many of which will be unsecured and using their default settings. Once a target has been identified the criminal can deploy a 'packet sniffer' which allows them to eavesdrop on any information that passes the compromised gateway. A packet sniffer is a device that intercepts data flowing in a network. You should also be aware that other malware can be deployed in the same way. This type of attack is virtually undetectable to the victims and can occur even in your 'secured' office environment without your knowledge.

AVOIDING PROBLEMS WITH MITM ATTACKS

4.10 You can reduce the risks of a MITM attack as follows:

- Avoid connecting to financial sites, online shops, files with personal details or commercially sensitive files through public networks.
- Don't allow your device to connect automatically to open networks. Make sure you only connect to known, trusted Wi-Fi networks.
- Invest in your own mobile hotspot for staff that regularly must work away from the office.
- Always use a Virtual Private Network (VPN) when connecting to unknown Wi-Fi networks.
- Encrypt your traffic and protect any sensitive information through strong passwords.
- Do not ignore website certificate warnings as these are a warning that something is amiss.
- Avoid websites that **do not** have HTTPS and the green padlock.

[8] SHODAN = Sentient Hyper-Optimised Data Access Network

- Whenever you finish connecting to a public network configure your device to 'forget' the network to prevent it constantly broadcasting SSIDs of networks you have connected to previously as these can be spoofed by a Wi-Fi Pineapple.
- Turn off your Wi-Fi functionality when you are not using it.
- Make sure all access points you control are secured and encrypted. Attackers that rely on physical proximity to deploy MITM attacks can be kept off a network by good security.
- Add a second authentication factor to any accounts that allow it.
- Make sure operating systems are updated to prevent MITM attacks that exploit system weaknesses.
- Install an up-to-date antivirus application and be sure it is set to scan your computer on a regular basis.
- Train your staff to keep an eye out for phishing attempts, or any email that requests requiring the users to click on a link to log in to a website. If users are unsure of the legitimacy of an email, they should navigate to the website in question manually and log in without using the email link. If they are still unsure, contact the organization that operates the site to see if it is a legitimate message.

4.11 If you are concerned that your organisation has been compromised by a keylogger or MITM attack report it to the NFIN helpline and if the attack is ongoing you may find 24/7 assistance there. To check whether you have been compromised or if you have been and you need to ensure that the compromise is terminated call in a specialist.

MISSED A PREVIOUS EDITION?

If you have missed a previous edition of the email campaign let us know and we can send you FREE a copy: contactus@profit.uk.com

1. Fraud Risks
2. Recruitment in Travel Fraud
3. Employee Fraud
4. Your Supply Chain
5. Upon Discovering A Fraud
6. Investigating A Fraud
7. When Police Become Involved
8. Preparing For Court
9. Validating A Booking
10. Payment Fraud Issues
11. Challenging A Chargeback
12. Other Payment Fraud
13. Protecting Images
14. Protecting Websites
15. DDOS Attacks & Hacking
16. Know Your Enemies
17. Spam & Malware
18. Other Ways Data Is Lost
19. Passwords

Like what we do to protect you?

We are always short of funds and need your support.

Find out how you can join PROFiT and fight fraud by emailing contactus@profit.uk.com

Next Week: Part 19 Passwords