The Threat of Ransomware + M365 Defense

The I.T. Team & ConnectingUp

the I.T. team™
Maintaining the health of your I.T. system

Connecting Up

What are we covering today?

- What is Ransomware?
- Ransomware Examples/Demo
- How to protect yourself
- Key protections within M365

About the I.T. team

- Formed in 2011
- Office 365 since its inception
- Managed Services/IT support
- A wide range of IT services
- Major NFP base of customers
- Providing IT services to NZ & Australian organisations

the I.T. team™

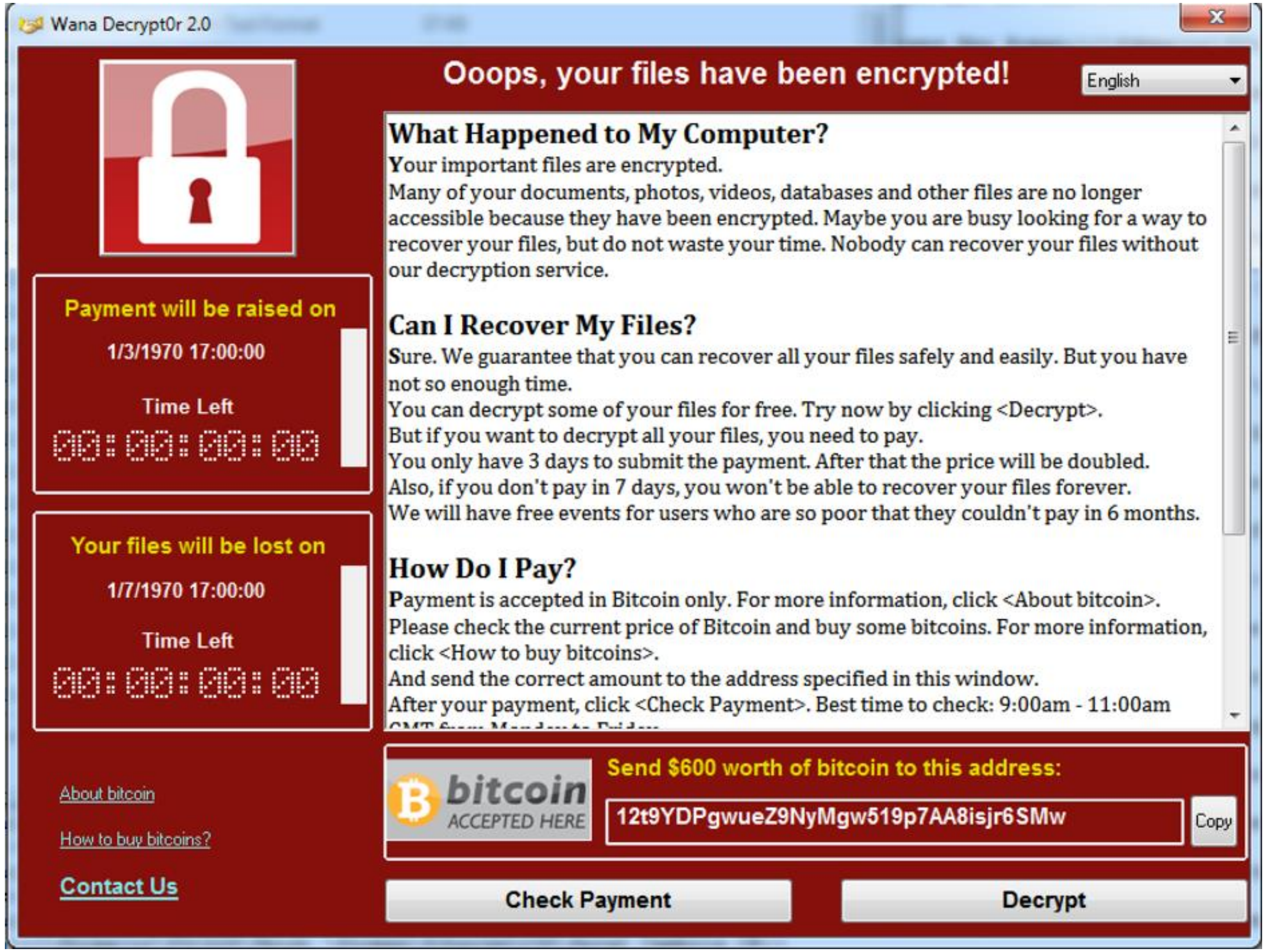
Maintaining the health of your I.T. system

Ransomware – The Rising Threat?

- Ransomware was biggest between 2010-2018
- Phishing has eclipsed Ransomware as dominant financial electronic crime
- Windows 10/11 has improved security, as has modern email protection
- EXE/MSI files blocked by default from email transmission
- Attachments heavily scrutinized
- Demands are increasing
- Leak threats are occuring
- AI may trigger a lift

What is Ransomware?

- Ransomware is a type of malicious software (malware) that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.



Ooops, your files have been encrypted!

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 GMT from Monday to Friday

Send $600 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

How Ransomware Works

- Hacker gains access
- Encrypts files (may take time)
- Notifies User/Requests Ransom

Ransomware Variants

- **WannaCry**: This ransomware caused a global outbreak in May 2017, exploiting a vulnerability in Microsoft's Server Message Block (SMB) protocol. It affected hundreds of thousands of computers in over 150 countries.
- **Petya/NotPetya**: Originally, Petya was a ransomware that encrypted the master file table (MFT) of the NTFS file system, making the entire system inaccessible. A later variant, known as NotPetya, was similar but designed more for destructive purposes than for collecting ransom.
- **Locky**: This ransomware was spread via malicious email attachments and was notable for its frequent changes in the method of encryption and obfuscation, making it harder to prevent.
- **Cerber**: Known for being offered as a Ransomware-as-a-Service (RaaS), Cerber encrypted files and then demanded a ransom. It was unique for its use of audio message to inform victims about the attack.
- **GandCrab**: This was another example of RaaS. GandCrab was updated rapidly over its life, with multiple versions appearing in a relatively short time frame, each version fixing flaws of the older ones and often changing encryption algorithms.
- **Sodinokibi/REvil**: The successor to GandCrab, this ransomware also adopted the RaaS model and has been associated with several high-profile attacks.
- **Ryuk**: Known for its targeted attacks, Ryuk has been a serious threat to large organizations and has often been linked to the TrickBot Trojan.
- **Dharma (CrySIS)**: Dharma ransomware, also known as CrySIS, is a family of ransomware that has been distributed in various ways, including through Remote Desktop Protocol (RDP) attacks.
- **Netwalker**: This ransomware, also known as Mailto, was used in attacks on healthcare providers during the COVID-19 pandemic.
- **Conti**: This ransomware uses a double extortion method - not only encrypting a victim's files but also threatening to publish stolen data unless a ransom is paid.

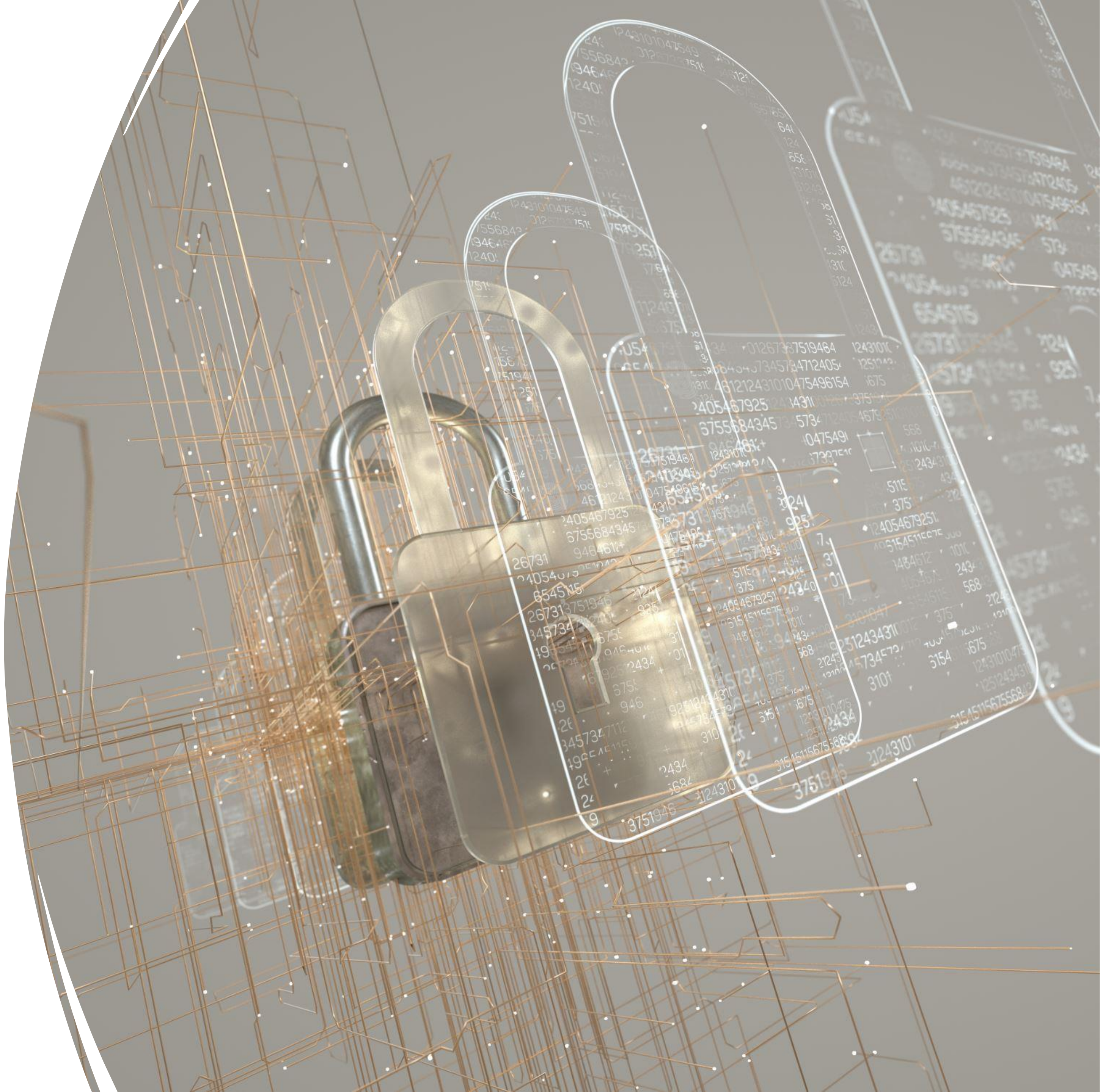
LIVE DEMO:

Ransomware Infection

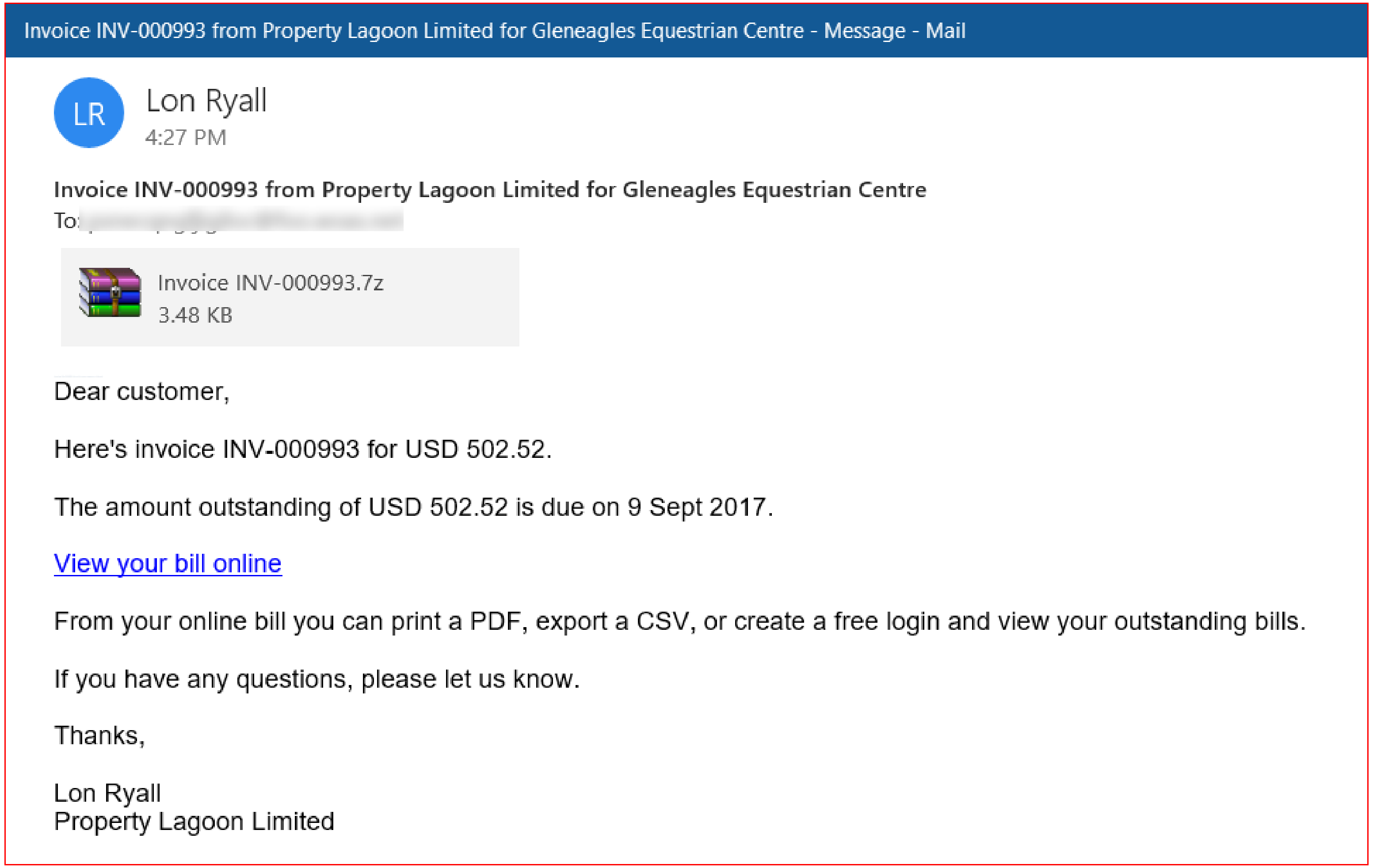
m² NETWORKS

How does it get in?

- Phishing (most common)
- Downloads (Torrent)
- Dodgy Websites
- 0-Day Vulnerability
- RDP Exploits



Phishing Example



Invoice INV-000993 from Property Lagoon Limited for Gleneagles Equestrian Centre - Message - Mail

Lon Ryall
4:27 PM

Invoice INV-000993 from Property Lagoon Limited for Gleneagles Equestrian Centre
To: [redacted]

Invoice INV-000993.7z
3.48 KB

Dear customer,

Here's invoice INV-000993 for USD 502.52.

The amount outstanding of USD 502.52 is due on 9 Sept 2017.

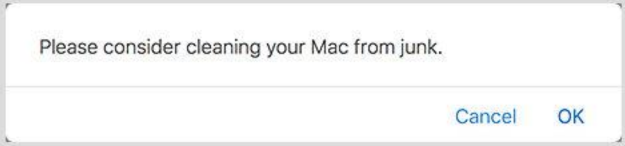
View your bill online

From your online bill you can print a PDF, export a CSV, or create a free login and view your outstanding bills.

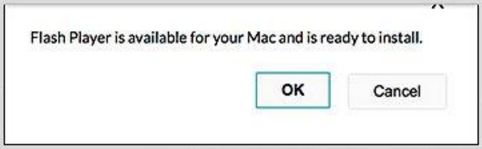
If you have any questions, please let us know.

Thanks,

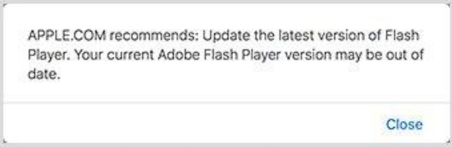
Lon Ryall
Property Lagoon Limited



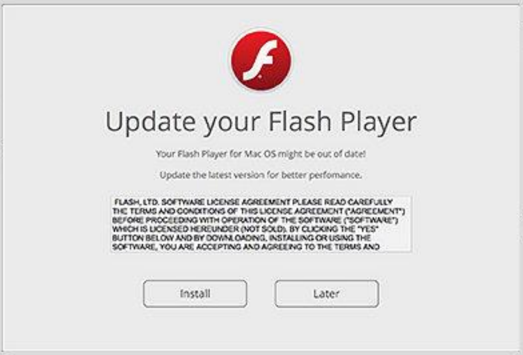
Please consider cleaning your Mac from junk.



Flash Player is available for your Mac and is ready to install.



APPLE.COM recommends: Update the latest version of Flash Player. Your current Adobe Flash Player version may be out of date.

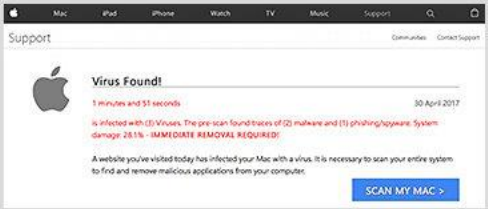


Update your Flash Player

Your Flash Player for Mac OS might be out of date!

Update the latest version for better perfomance.

FLASH, LTD. SOFTWARE LICENSE AGREEMENT PLEASE READ CAREFULLY THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT ("AGREEMENT") BEFORE PROCEEDING WITH OPERATION OF THE SOFTWARE ("SOFTWARE") WHICH IS LICENSED HEREUNDER (NOT SOLD). BY CLICKING THE "YES" BUTTON BELOW AND BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE, YOU ARE ACCEPTING AND AGREEING TO THE TERMS AND

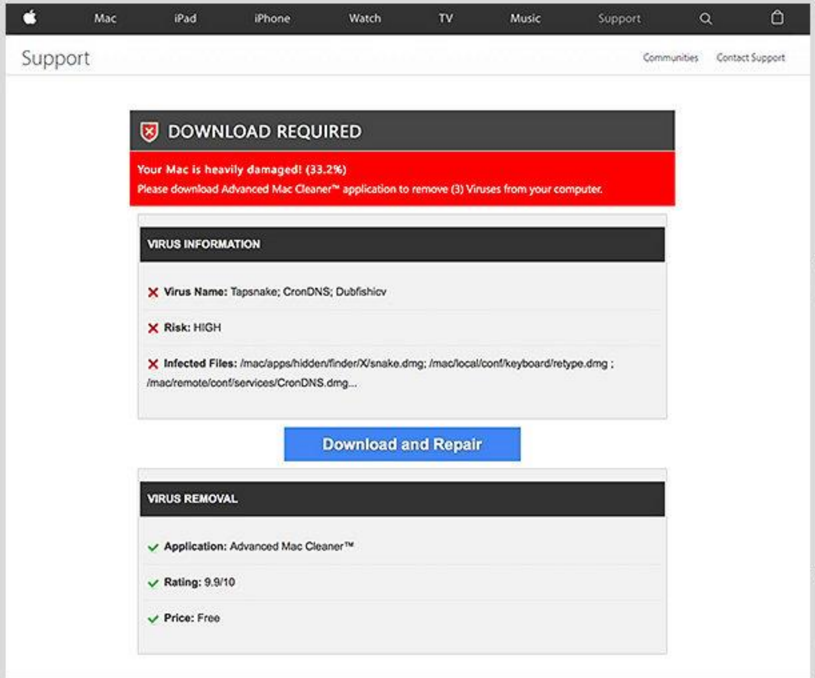


Virus Found!

1 minutes and 51 seconds 30 April 2017

is infected with (3) Viruses. The pre-scan found traces of (2) malware and (1) phishing/spyware. System damage: 28.1% - IMMEDIATE REMOVAL REQUIRED!

A website you've visited today has infected your Mac with a virus. It is necessary to scan your entire system to find and remove malicious applications from your computer.



DOWNLOAD REQUIRED

Your Mac is heavily damaged! (33.2%)

Please download Advanced Mac Cleaner™ application to remove (3) Viruses from your computer.

VIRUS INFORMATION

✗ **Virus Name:** Tapsnake; CronDNS; Dubfishicv

✗ **Risk:** HIGH

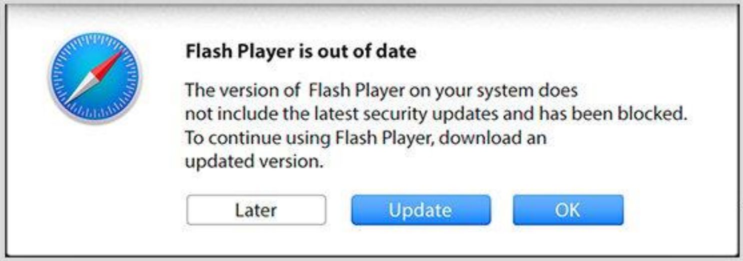
✗ **Infected Files:** /mac/apps/hidden/finder/X/snake.dmg; /mac/local/conf/keyboard/retype.dmg ; /mac/remote/conf/services/CronDNS.dmg...

VIRUS REMOVAL

✓ **Application:** Advanced Mac Cleaner™

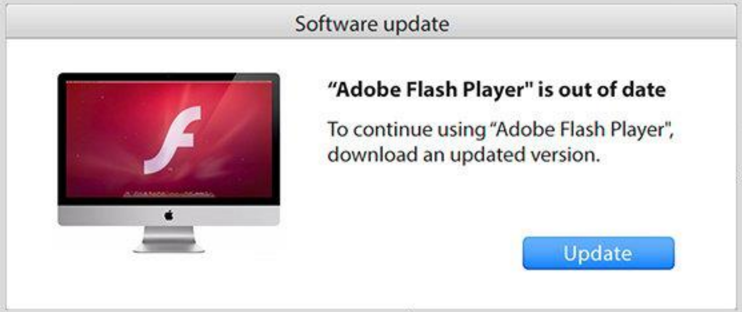
✓ **Rating:** 9.9/10

✓ **Price:** Free



Flash Player is out of date

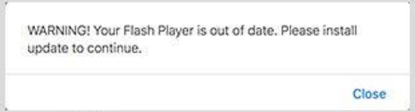
The version of Flash Player on your system does not include the latest security updates and has been blocked. To continue using Flash Player, download an updated version.



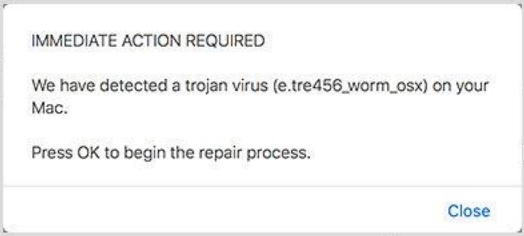
Software update

"Adobe Flash Player" is out of date

To continue using "Adobe Flash Player", download an updated version.



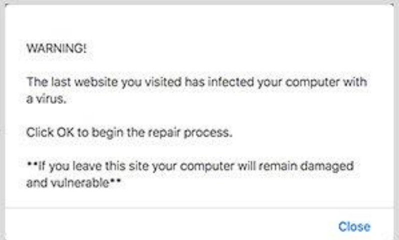
WARNING! Your Flash Player is out of date. Please install update to continue.



IMMEDIATE ACTION REQUIRED

We have detected a trojan virus (e.tre456_worm_osx) on your Mac.

Press OK to begin the repair process.

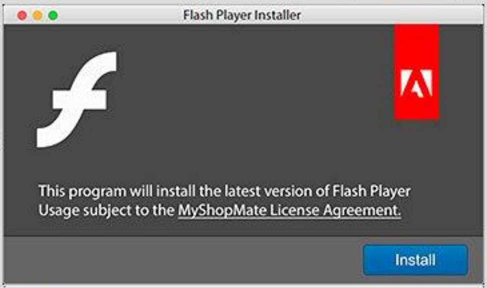


WARNING!

The last website you visited has infected your computer with a virus.

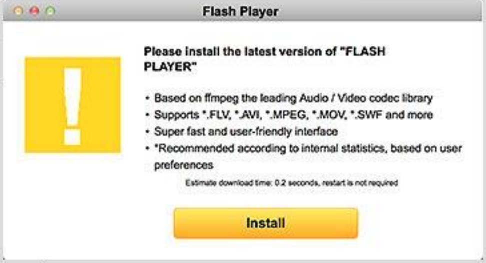
Click OK to begin the repair process.

If you leave this site your computer will remain damaged and vulnerable



Flash Player Installer

This program will install the latest version of Flash Player
Usage subject to the MyShopMate License Agreement.

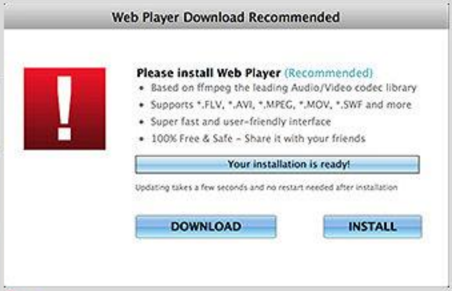


Flash Player

Please install the latest version of "FLASH PLAYER"

- Based on ffmpeg the leading Audio / Video codec library
- Supports *.FLV, *.AVI, *.MPEG, *.MOV, *.SWF and more
- Super fast and user-friendly interface
- *Recommended according to internal statistics, based on user preferences

Estimate download time: 0.2 seconds, restart is not required



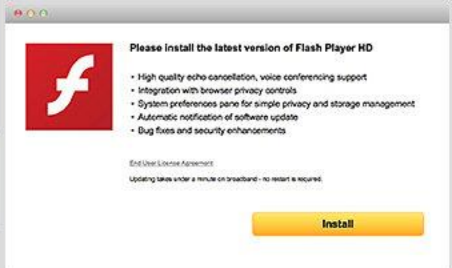
Web Player Download Recommended

Please install Web Player (Recommended)

- Based on ffmpeg the leading Audio/Video codec library
- Supports *.FLV, *.AVI, *.MPEG, *.MOV, *.SWF and more
- Super fast and user-friendly interface
- 100% Free & Safe – Share it with your friends

Your installation is ready!

Updating takes a few seconds and no restart needed after installation

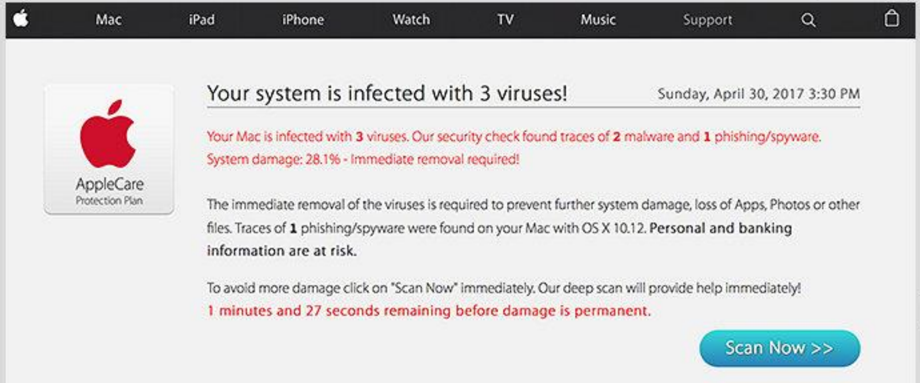


Please install the latest version of Flash Player HD

- High quality echo cancellation, voice conferencing support
- Integration with browser privacy controls
- System preferences pane for simple privacy and storage management
- Automatic notification of software update
- Bug fixes and security enhancements

End User License Agreement

Updating takes under a minute on broadband - no restart is required.

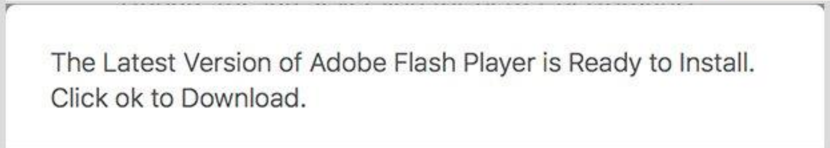


Your system is infected with 3 viruses! Sunday, April 30, 2017 3:30 PM

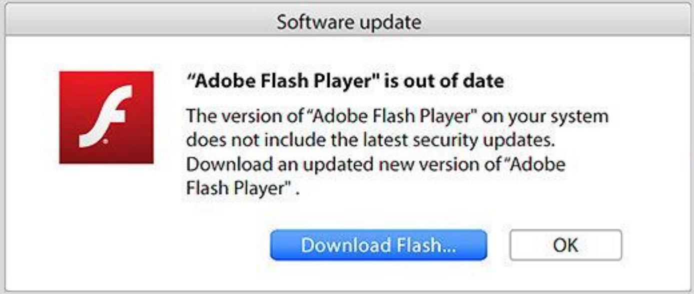
Your Mac is infected with 3 viruses. Our security check found traces of 2 malware and 1 phishing/spyware. System damage: 28.1% - Immediate removal required!

The immediate removal of the viruses is required to prevent further system damage, loss of Apps, Photos or other files. Traces of 1 phishing/spyware were found on your Mac with OS X 10.12. Personal and banking information are at risk.

To avoid more damage click on "Scan Now" immediately. Our deep scan will provide help immediately!
1 minutes and 27 seconds remaining before damage is permanent.



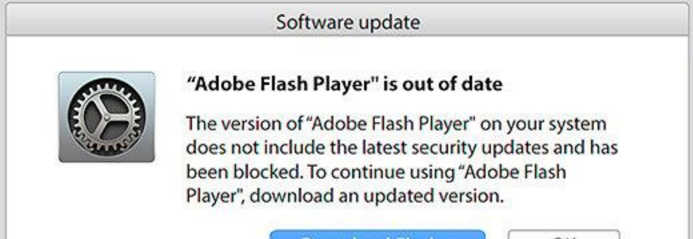
The Latest Version of Adobe Flash Player is Ready to Install.
Click ok to Download.



Software update

"Adobe Flash Player" is out of date

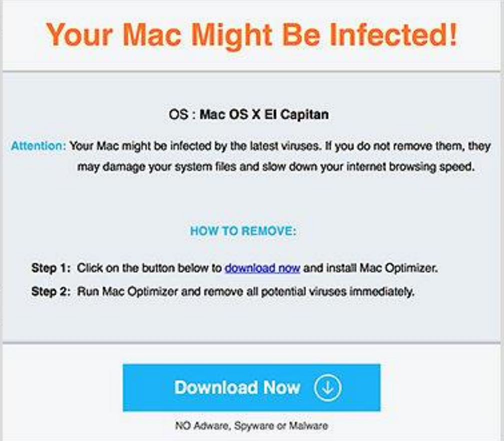
The version of "Adobe Flash Player" on your system does not include the latest security updates. Download an updated new version of "Adobe Flash Player" .



Software update

"Adobe Flash Player" is out of date

The version of "Adobe Flash Player" on your system does not include the latest security updates and has been blocked. To continue using "Adobe Flash Player", download an updated version.



Your Mac Might Be Infected!

OS : Mac OS X El Capitan

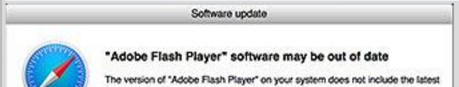
Attention: Your Mac might be infected by the latest viruses. If you do not remove them, they may damage your system files and slow down your internet browsing speed.

HOW TO REMOVE:

Step 1: Click on the button below to download now and install Mac Optimizer.

Step 2: Run Mac Optimizer and remove all potential viruses immediately.

NO Adware, Spyware or Malware

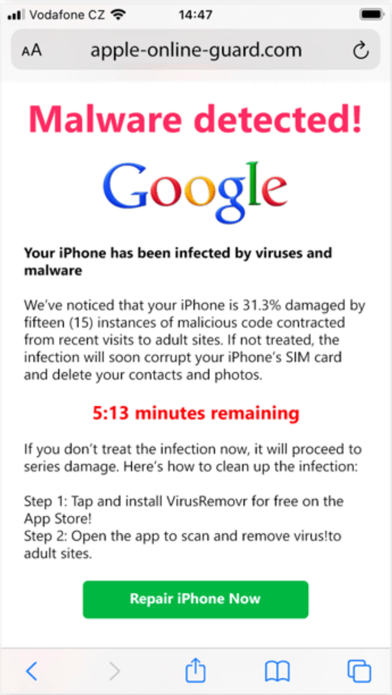


Software update

"Adobe Flash Player" software may be out of date

The version of "Adobe Flash Player" on your system does not include the latest

Scareware



Malware detected!

Google

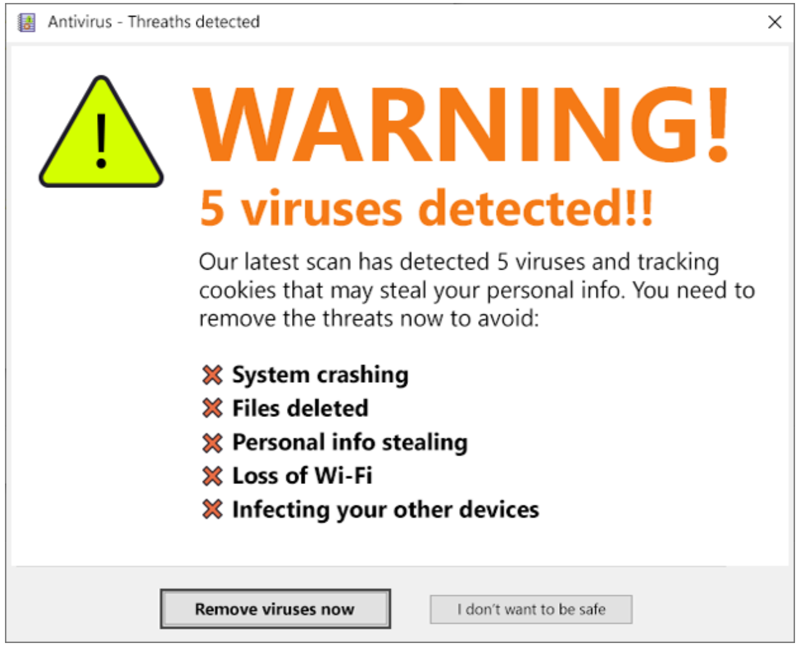
Your iPhone has been infected by viruses and malware

We've noticed that your iPhone is 31.3% damaged by fifteen (15) instances of malicious code contracted from recent visits to adult sites. If not treated, the infection will soon corrupt your iPhone's SIM card and delete your contacts and photos.

5:13 minutes remaining

If you don't treat the infection now, it will proceed to series damage. Here's how to clean up the infection:

Step 1: Tap and install VirusRemovr for free on the App Store!
Step 2: Open the app to scan and remove virus!to adult sites.

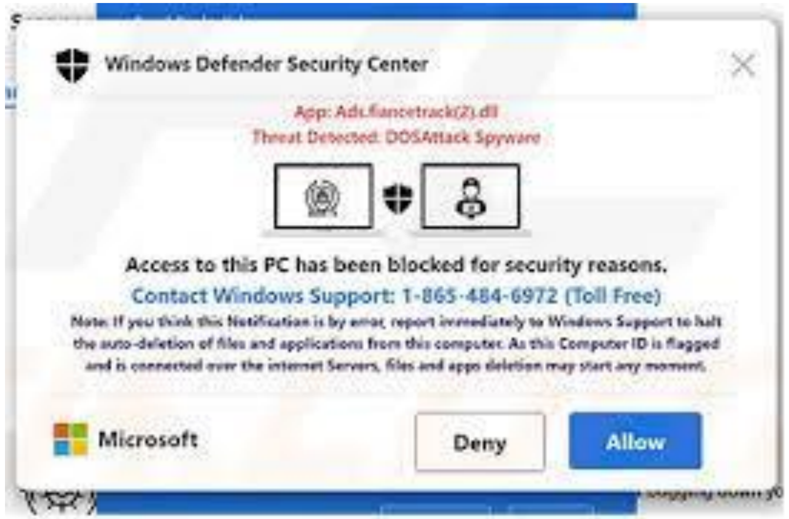


WARNING!

5 viruses detected!!

Our latest scan has detected 5 viruses and tracking cookies that may steal your personal info. You need to remove the threats now to avoid:

- ✖ **System crashing**
- ✖ **Files deleted**
- ✖ **Personal info stealing**
- ✖ **Loss of Wi-Fi**
- ✖ **Infecting your other devices**



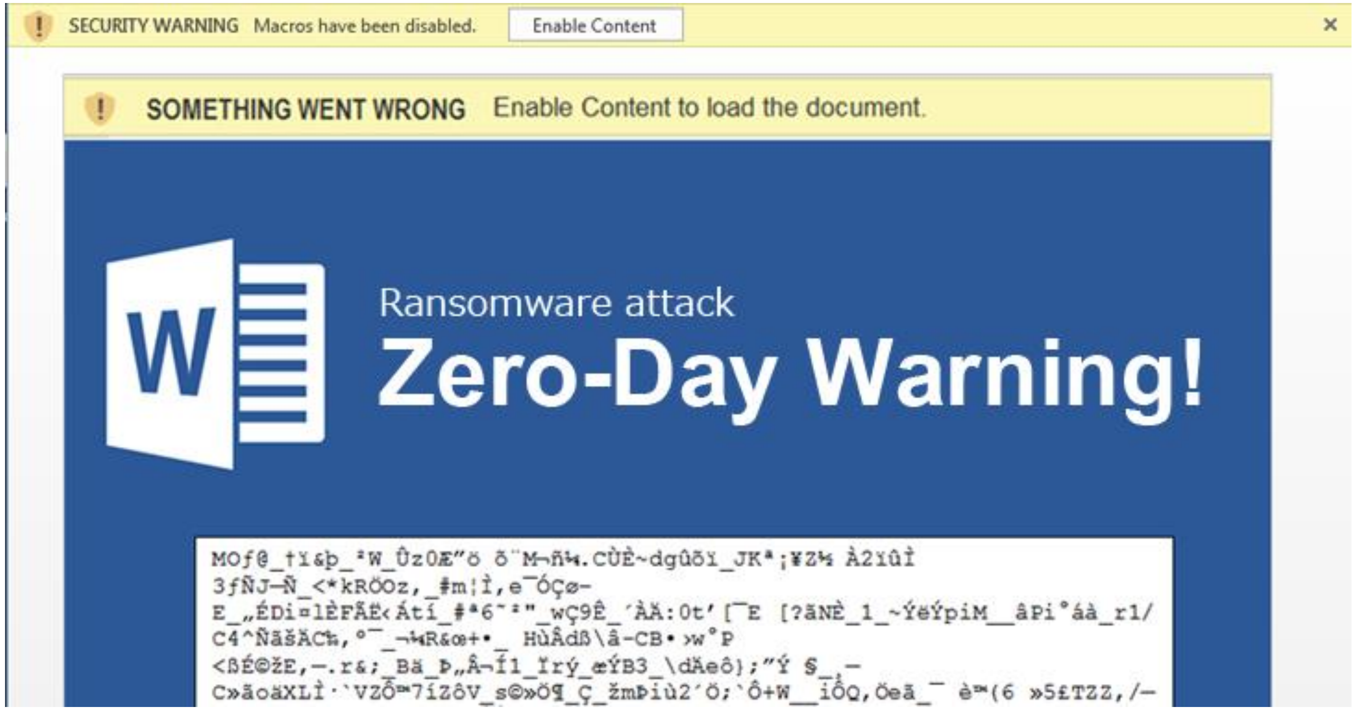
App: Ads.fiancetrack(2).dll
Threat Detected: DOSAttack Spyware

Access to this PC has been blocked for security reasons.

Contact Windows Support: 1-865-484-6972 (Toll Free)

Note: If you think this Notification is by error, report immediately to Windows Support to halt the auto-deletion of files and applications from this computer. As this Computer ID is flagged and is connected over the internet Servers, files and apps deletion may start any moment.

Zero Day



SECURITY WARNING Macros have been disabled.

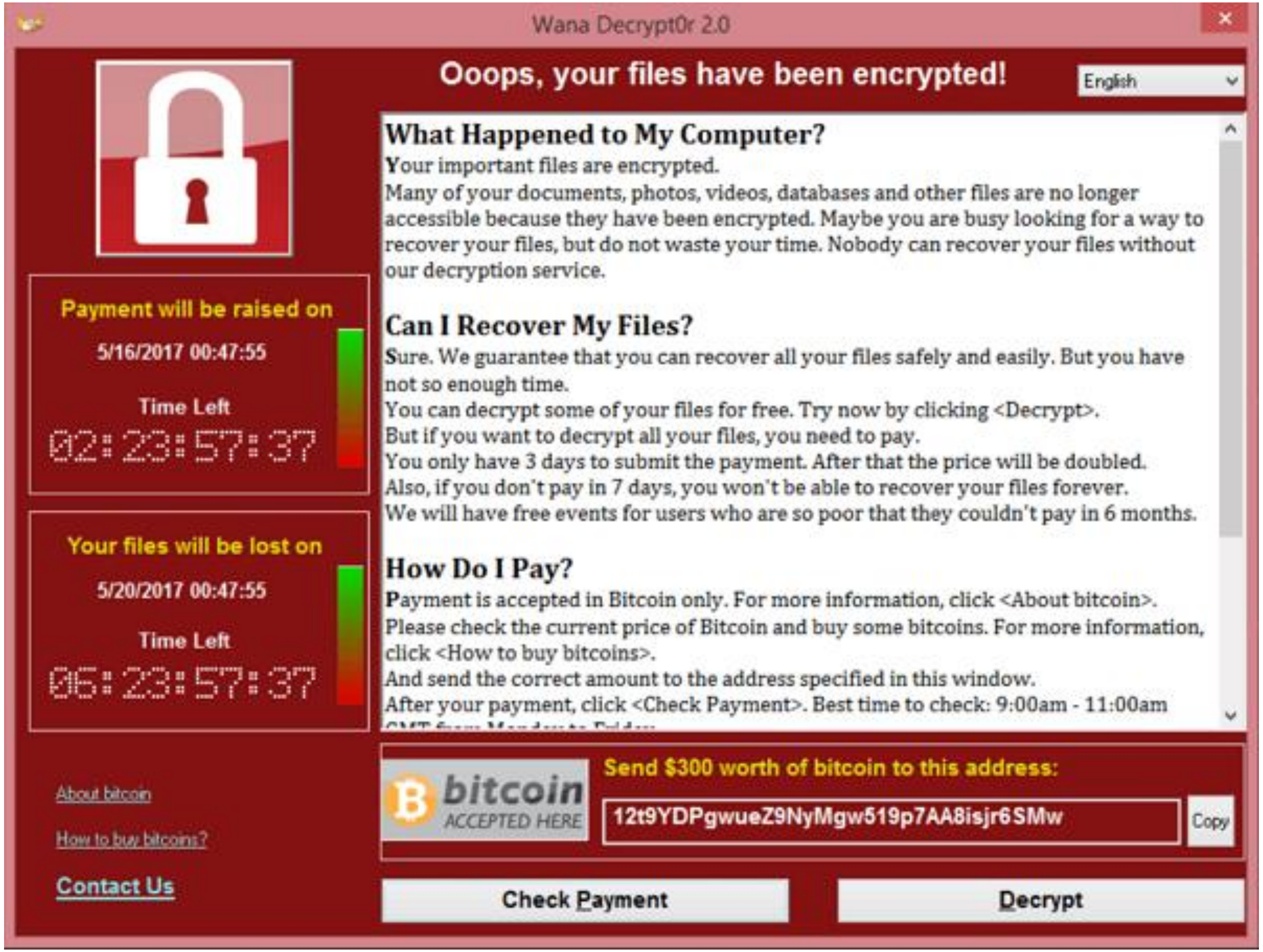
SOMETHING WENT WRONG Enable Content to load the document.

Ransomware attack

Zero-Day Warning!

```
MOf@_†Ĭ&þ_²W_Ûz0Æ”ö õ¨M¬ñ¼.CÙÈ~dgûõĭ_JKª;¥Z½ À2ĭûÌ
3ƒÑJ—Ñ_<*kRÖOz,_#m¦Ì,e¯ÓÇø-
E_„ÉDi¤lÈFÃÆ‹Átí_#ª6˜²"_wÇ9Ê_´ÀÄ:0t’[¯E [?ãNÈ_1_~ÝëÝpiM__âÞi°áà_r1/
C4^ÑăšÄC‰,°¯_¬¼R&œ+•_ HùÂdß\â-CB•›w°P
<ßÉ©žE,—.r&;_Bă_Þ„Â¬Ĩ1_Ĭrý_æÝB3_\dÄeô};”Ý §_¸—
C»ãoäXLÌ·`VZŌ™7íZôV_s©»Ö¶_Ç_žmÞiù2´Ö;`Ô+W__iÔQ,Öeã_¯ è™(6 »5£TZZ,/—
```

Example



Ooops, your files have been encrypted!

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 GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

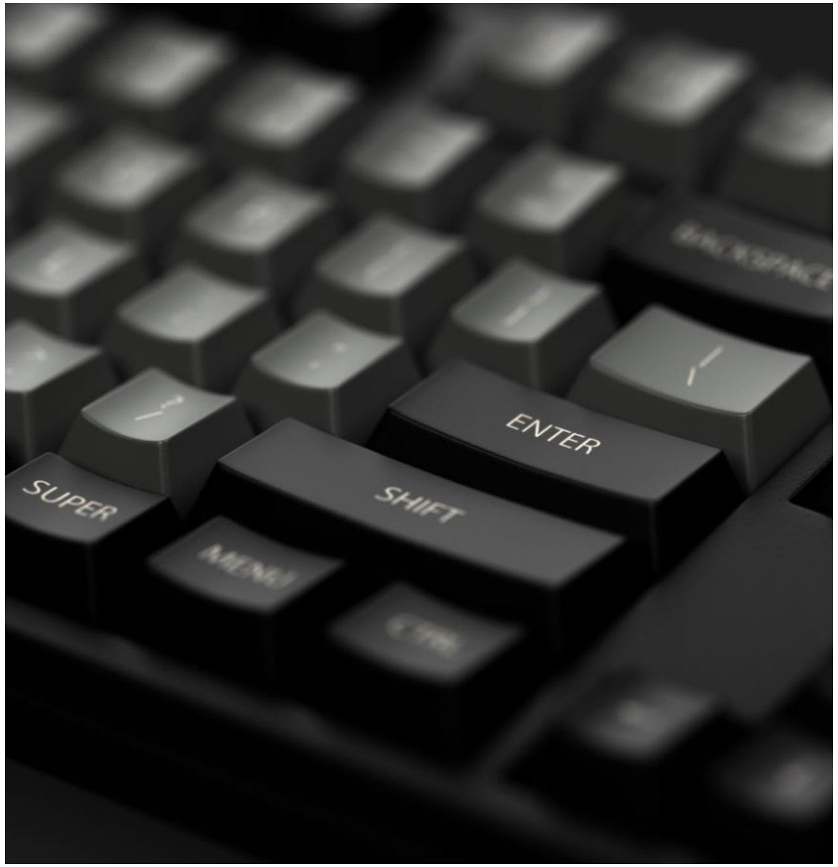
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Recognising the Warning Signs

- Dodgy looking emails or websites
- Attachment you open that doesn’t seem to work
- Very slow device, unexpectedly
- Potential popups from Anti-Malware products
- Files inaccessible, unusual writing
- New Text Files on desktop/documents or Background altered

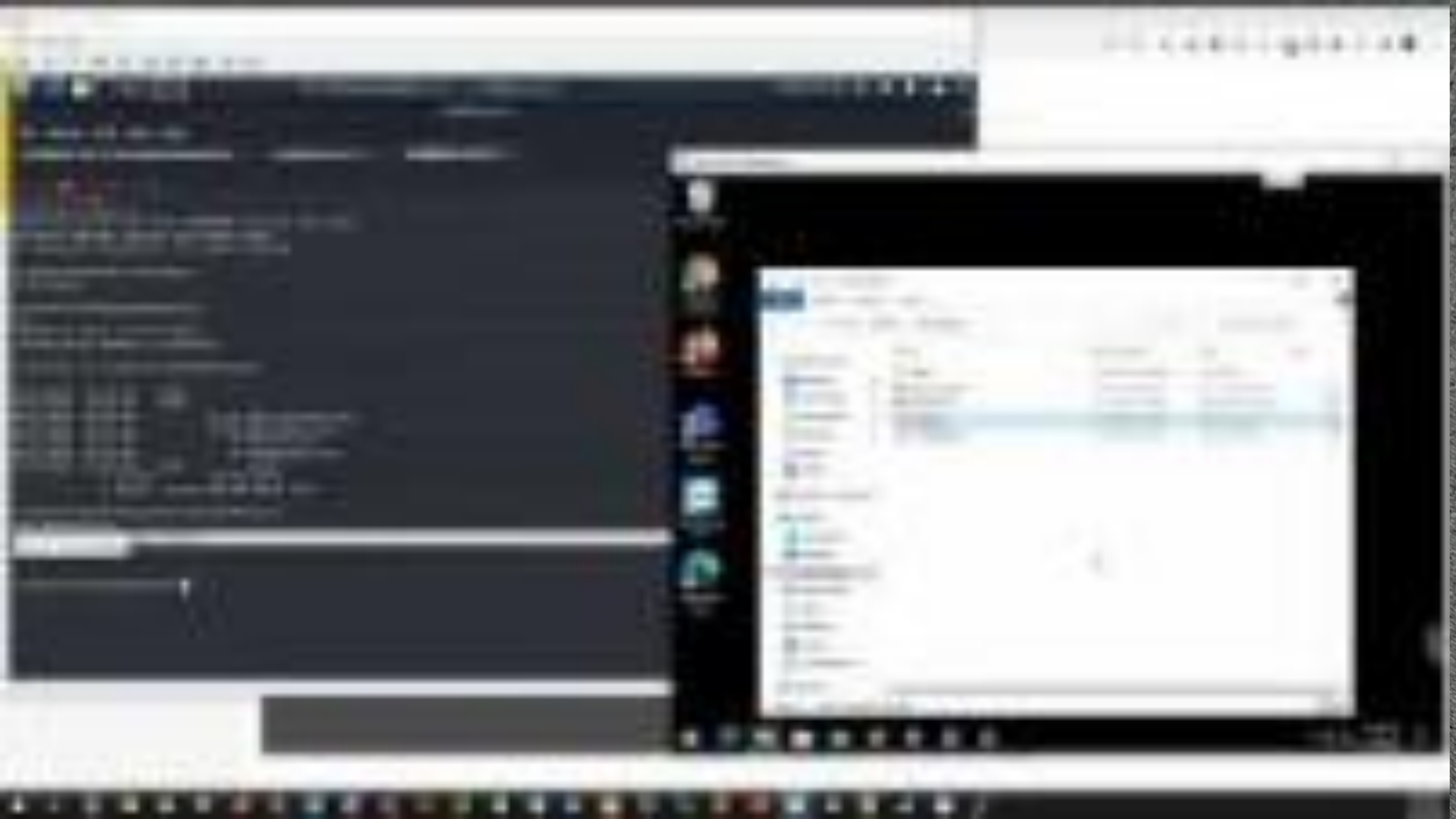
Protection/Prevention (pt 1)

- Backups
  - Third party SAAS Backup
  - OneDrive/Google Drive/DropBox etc
  - Potentially an Airgap backup
  - Server Backup if required (multiple)
- Strong Email Filtering, well configured
- Endpoint Protection



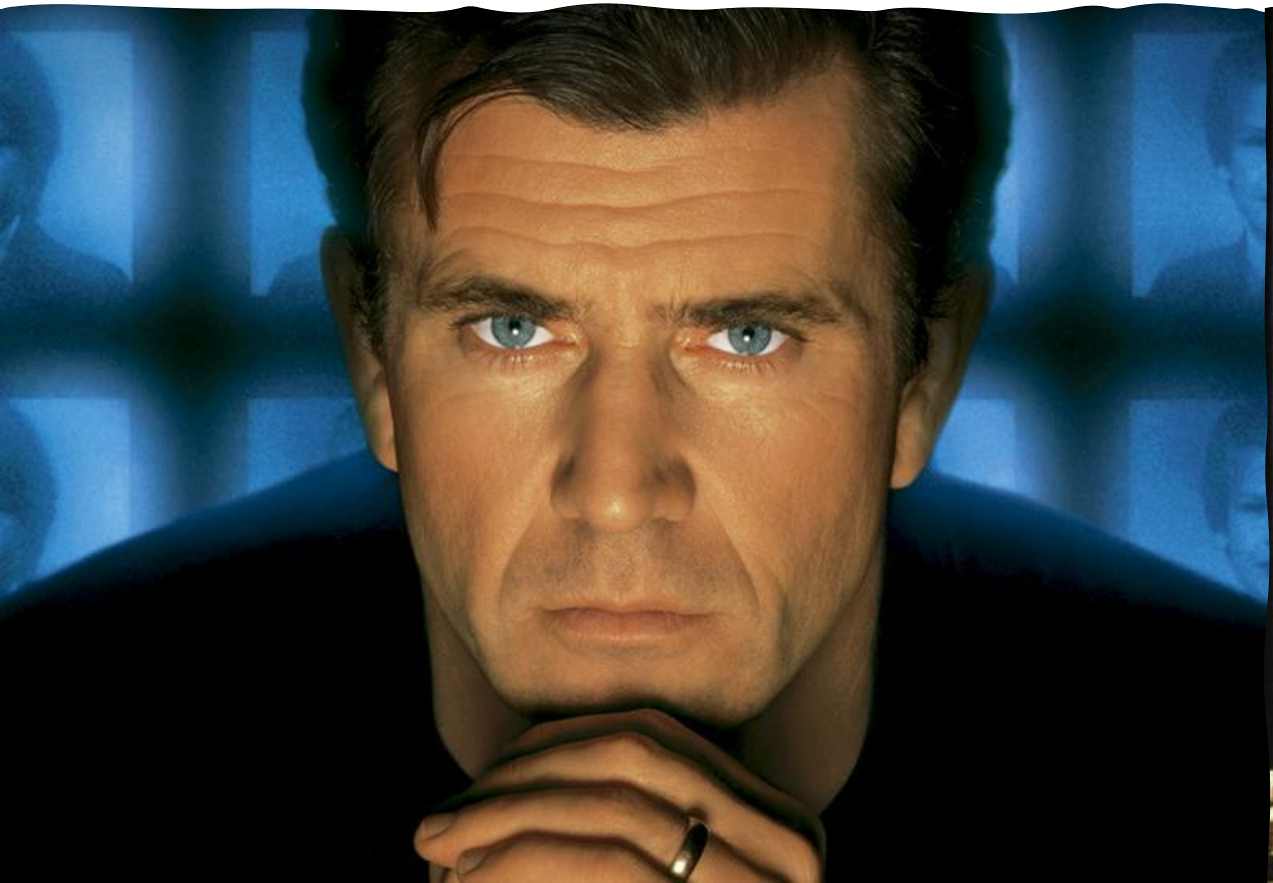
Protection/Prevention (pt 2)

- System Updates
  - 0 – day vulnerabilities need to be jumped on quickly
- Protection against Phishing
- Protection against Dodgy Websites
- Firewall – configured to block certain ports
- User Guidance



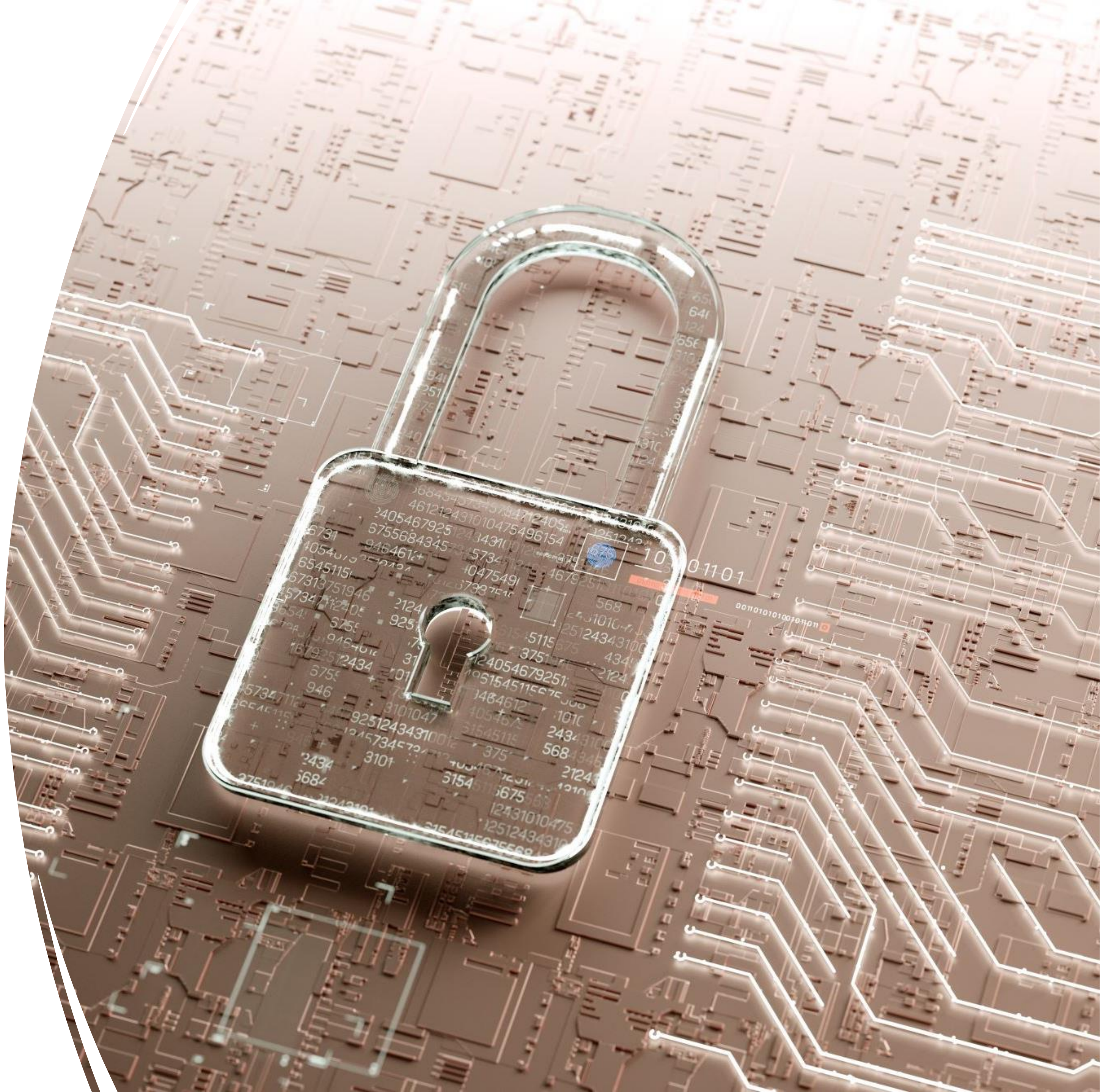
Ransom

- Can you pay the ransom?
- Will you get your files back?
- Should you pay the ransom?



Microsoft 365

- M365 is increasingly improving its security protections



What does Base 365 do to protect you?

- Forefront – Basic Email filtering, will protect you against the key threats
- Windows Defender – decent if not brilliant protection on your device
- Sharepoint/OneDrive – protection built in
- Recycle bin – Backups don't exist but rollback does occur
- Windows significantly more secure than 10 years ago

What advanced functions exist to protect you?

- Defender for 365 (ATP)
  - Available in Business Premium or specific licenses
  - Better protection against Phishing, Malware, etc
  - Allows Advanced Quarantine
  - Tooltups (Security Labels on emails)
- Defender for Endpoint
  - Built upon Windows Defender
  - Advanced Protection and alerting
  - Higher License types have heavy protection
- Defender – Advisories
  - Notifications of major threats that may require intervention
- Standard functions such as MFA, Conditional Access etc will improve your protection

Additional Protections

- Advanced SOC/SIEM service
  - RocketCyber
  - Huntress
  - SKOUT
- Advanced Endpoint Protection
  - SentinelOne
  - CrowdStrike
- Third Party 365 Backup
- Patch Management
- Server Backups/Airgap

AI

Whats next?

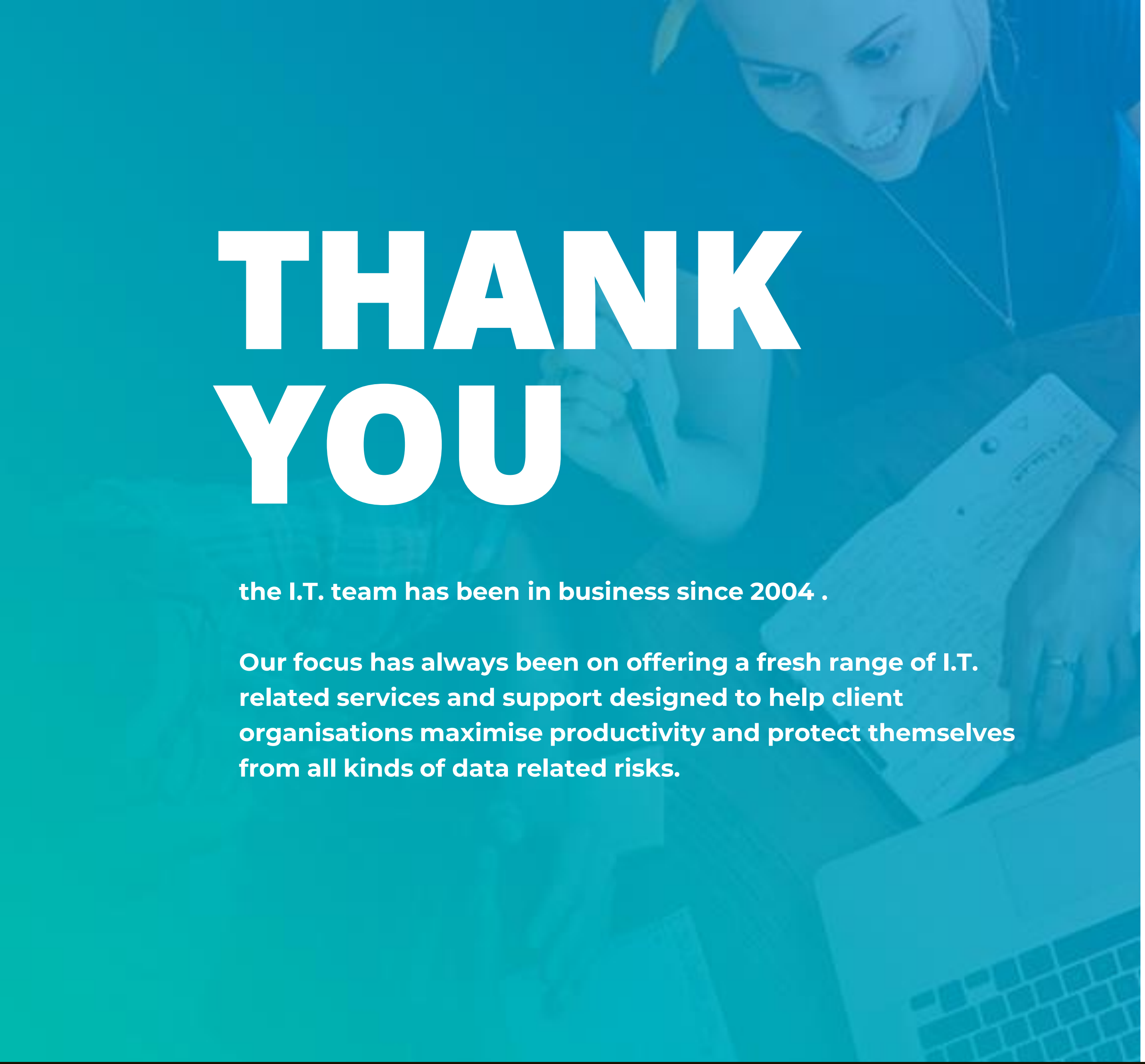
Where to from here?

- Assess your current situation
- Determine your highest risk
- Create a plan
- Delve deeper into 365

the I.T. team™
Maintaining the health of your I.T. system

QUESTION TIME

webinar@theitteam.co.nz



THANK YOU

the I.T. team has been in business since 2004 .

Our focus has always been on offering a fresh range of I.T. related services and support designed to help client organisations maximise productivity and protect themselves from all kinds of data related risks.

the I.T. team™

Maintaining the health of your I.T. system

theitteam.co.nz