

These notes will cover 4 sections  
Use the RIGHT arrow key to go to the next slide  
Use the LEFT arrow key to go back a slide

- 1 Crypto Locker – recent ransom malware
- 2 Action Centre in Windows Control Panel (Win 7 and Win 8)
- 3 Windows Firewall
- 4 Anti- Virus / Anti- Malware programs and an assessment of their relative merits

# CRYPTOLOCKER

## Your personal files are encrypted!



Private key will be destroyed on  
12/1/2013  
10:18 AM

Time left  
**42 : 48 : 44**

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt the files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

**To obtain** the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR / similar amount** in another currency.

Click «Next» to select the method of payment.

**Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.**

Next >>

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key [RSA-2048](#) generated for this computer. To decrypt the files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

**To obtain** the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR / similar amount** in another currency.

Click «Next» to select the method of payment.

**Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.**

The main targets of the cryptolocker criminals are businesses as they probably panic and pay.  
Bit Coin seems a favourite payment method

The techniques used to infect your computer are the same for most Malware.

I will use examples I have found over the last few weeks  
After the slide on Bit Coin

## **Payment using BitCoin**

Is a preferred ransom payment method for Cryptolocker.

Bitcoins are similar to travellers cheques but are a digital money traded over the internet but are hard to trace and unregulated by governments.

Bitcoins have operated since 2009 and work on fee per transaction like a Travellers Cheque. They offer an “exchange” rate between internationally recognised currencies. You buy bitcoins and transmit them to a recipient who later uses them for other transactions or converts them into recognised currency.

Bitcoin ATM machines exist.

The “exchange” rate is highly volatile.

# How do computers become infected with Cryptolocker

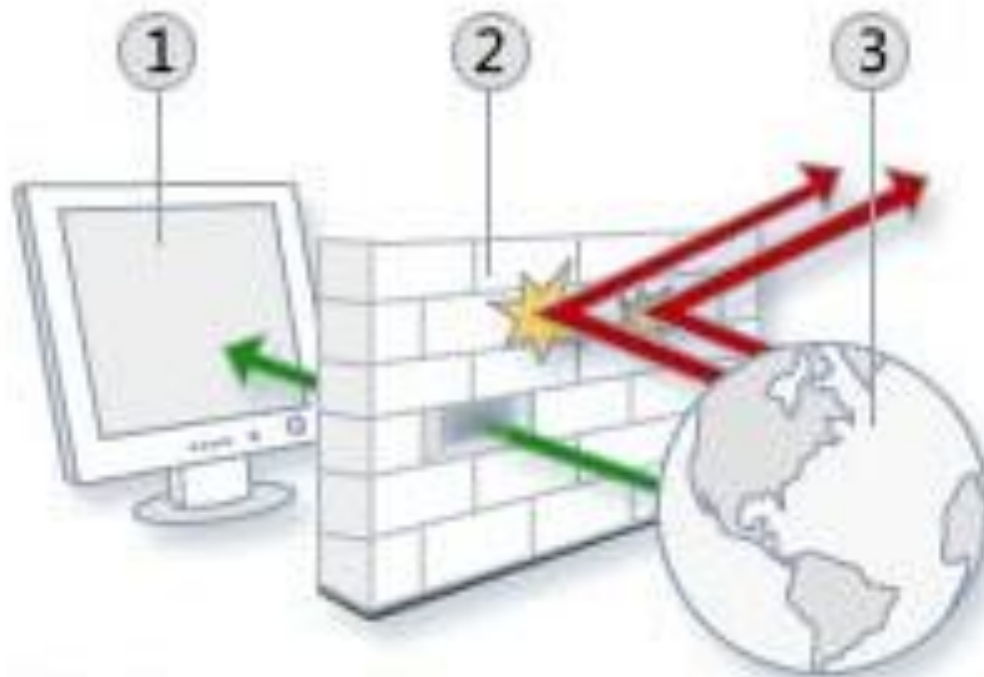
The principle requirements are :

1. Out of date Anti Virus / Anti Malware or Windows Updates
2. Tricks to make you to defeat the Firewall.
3. Access to On-Line backup files as well as current files.

Opening an Email attachment (often made to look like a PDF file) that has the Cryptolocker program hidden in the attachment.

Or tricking you to click a link that downloads the malware.

The first defence that malware has to get past is the Firewall



- ① Your computer
- ② Your firewall
- ③ The Internet

An Email message is permitted to pass both in and out a firewall  
You have to be tricked into opening the Email or Attachment

The Email seems to come from a reputable source  
and is addressed to you personally.

(The Email style has been carefully counterfeited to look genuine)

(The offer is too good to be true)

(It may be a business action or report that is not suspicious)

I have copied a few Emails that just about fill the bill from my  
OUTLOOK 2010 Junk Mail folder.

## CONFIRMATION SECURITY MESSAGE - ANZ Bank

ANZ <e-confirmation@anz.co.nz>

Links and other functionality have been disabled in this message. To restore functionality, move this message to the Inbox.  
This message was marked as spam using the Outlook Junk E-mail filter.  
This message was sent with High importance.  
This message was converted to plain text.

Sent: Mon 20/01/2014 2:27 a.m.

To: 

CONFIRMATION SECURITY MESSAGE

Banks don't communicate like this

Happy week ahead ANZ customer.

Joining ANZ bank has prompted ANZ team to keep eye of your money and make sure you are secured so due to this,

it's strongly required that you should Validate your logon and security Details.

VALIDATE YOUR ACCOUNT HERE

<<http://devonportchurches.org.au/templates/system/images/secure.anz.co.nz/IBCS/pgLogin/>>

Not https, and an irrelevant Australian site

This email was sent automatically please do not respond just click the link to update

Copyright 2014 © ANZ Bank New Zealand Limited. All rights reserved.

## ANZ Bank Online Customers Security Notification!

ANZ Bank <service@anz.co.nz>

- Links and other functionality have been disabled in this message. To restore functionality, move this message to the Inbox.  
This message was marked as spam using the Outlook Junk E-mail filter.  
Extra line breaks in this message were removed.  
This message was converted to plain text.

Sent: Fri 24/01/2014 7:19 a.m.

To: Recipients

ANZ Bank Online Customers Security Notification!

Banks don't communicate like this

Due to a recent upgrade in our server, we are currently reviewing member's account and we request you to please take just a second out of your time to comply with this upgrade for effect on your account,

Not https and comes from Thailand


Please Click Here To Start <<http://www.tourindy.co.th/images/Logon.php>>

Failure to comply might lead to suspension or problem accessing your account.

Thank you for using ANZ Banking Group Limited.

## Account Protection Message.

ANZ Bank <e-bank@anz.co.nz>

 Links and other functionality have been disabled in this message. To restore functionality, move this message to the Inbox. This message was marked as spam using the Outlook Junk E-mail filter. This message was converted to plain text.

Sent: Sat 25/01/2014 5:19 a.m.

To: 

Good Day ANZ customer

**Banks don't communicate like this**

we are informing you to follow the link below to update your internet login details due to some possible internet complications for safety purpose:

**Not https and comes from an irrelevant site**

ANZ VERIFY LINK <<http://powerbeaminc.com/image/secure.anz.co.nz/IBCS/pgLogin/>>

We Live In Your World - ANZ

Copyright 2014 Â© ANZ Bank New Zealand Limited. All rights reserved.

Powered by Google

Comes from Kenya

Google Corporation® <josephine.irungu@holmes.co.ke>

Links and other functionality have been disabled in this message. To restore functionality, move this message to the Inbox.  
This message was marked as spam using the Outlook Junk E-mail filter.  
Extra line breaks in this message were removed.  
Outlook blocked access to the following potentially unsafe attachments: Google UK.pdf.



Suspicious attachment

Sent: Fri 24/01/2014 8:56 a.m.

To:

Dear Google User,

You have been selected as a winner for using Google services. Find attached email with more details.

Congratulations,

Matt Brittin.

CEO Google UK.

©2014 Google Incorporation®

## Powered By Google

Google Incorporation® <qhalil@cidb.gov.my> **Now moved to Malaysia**

- Links and other functionality have been disabled in this message. To restore functionality, move this message to the Inbox.  
This message was marked as spam using the Outlook Junk E-mail filter.  
Extra line breaks in this message were removed.  
Outlook blocked access to the following potentially unsafe attachments: Google.pdf.

Sent: Thu 16/01/2014 8:50 a.m.

To:

---


Dear Google User,

You have been selected as a winner for using Google services. Find attached email with more details.

Congratulations,

Matt Brittin.  
CEO Google UK.

©2013 Google Incorporation®

 Links and other functionality have been disabled in this message. To restore functionality, this message was marked as spam using the Outlook Junk E-mail filter. This message was converted to plain text.

From: A Ken <hayesc@cf.edu>  
To: Undisclosed recipients:  
Cc:  
Subject: Swift Copy Of Payment

From Central African Republic  
And Suspicious attachment

Hello,

Please find attached swift copy of payment.

<[http://mindviz.com/gfx/attach\\_icon.gif](http://mindviz.com/gfx/attach_icon.gif)> 1 Attached files | 125KB


\$131,085.pdf <<http://www.cameroun50.cm/media/wire.php>>

Await soonest reply.

Regards

A Ken

Sales Manager



 Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: ANZ BANK <amycbaker@aol.com>

To: 

Cc:

Subject: ANZ Status Update !!

 Message  ANZ REWARD.html (8 KB)



Congratulations,

For using your ANZ Debit and Cheque Card, you earn 10% back of your spending.

Download Attachment to activate your Rewards and it will reflect on your account every month end.

ANZ Rewards is a revolutionary loyalty programme that rewards you whenever you use your ANZ Debit, Cheque or Credit Card - up to 10% back - no matter where you shop. What's more, earn up to 10%

---

Receive, review, pay and organize all your bills online.

Alert: (215934610)

Document Reference: (87906628)

# Ensuring you have the best security defences

Apart from being vigilant on opening attachments  
or following Email highlighted links  
we can use a range of security features to improve our defences

The following slides are based on Windows 7 and Windows 8

As I no longer have access to XP I could not verify the relevance to XP.

The Control Panel gives access  
to

Action Centre  
Windows Defender  
Windows Firewall

Adjust your computer's settings



Action Center



Administrative Tools



Credential Manager



Date and Time



Devices and Printers



Display



Region and Language



RemoteApp and Desktop Connections



System









Taskbar and Start Menu



Windows Defender



Windows Firewall

-  Action Center
-  Credential Manager
-  Devices and Printers
-  Administrative Tools
-  Date and Time
-  Display

- Control Panel Home
-  Change Action Center settings
-  Change User Account Control settings
- View archived messages
- View performance information

## ACTION CENTRE SETTINGS

### Turn messages on or off

For each selected item, Windows will check for problems and send you a message if problems are found.  
How does Action Center check for problems?

#### Security messages

---

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Windows Update             | <input checked="" type="checkbox"/> Spyware and related protection |
| <input checked="" type="checkbox"/> Internet security settings | <input checked="" type="checkbox"/> User Account Control           |
| <input checked="" type="checkbox"/> Network firewall           | <input checked="" type="checkbox"/> Virus protection               |

#### Maintenance messages

---


- |   |   |
|---|---|
| <input type="checkbox"/> Windows Backup                     | <input checked="" type="checkbox"/> Check for updates |
| <input checked="" type="checkbox"/> Windows Troubleshooting |   |

- Action Center
- Credential Manager
- Devices and Printers
- Administrative Tools
- Date and Time
- Display

- Control Panel Home
- Change Action Center settings
- Change User Account Control settings
- View archived messages
- View performance information

Control Panel Home

Change Action Center settings

 Change User Account Control settings

View archived messages

View performance information


## Review recent messages and resolve problems

No issues have been detected by Action Center.

## USER ACCOUNT CONTROL

### Security

Network firewall On

 Windows Firewall is actively protecting your computer.

Windows Update On

Windows will automatically install updates as they become available.

Virus protection On

Microsoft Security Essentials reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

Microsoft Security Essentials reports that it is turned on.

[View installed antispymware programs](#)

Internet security settings OK

All Internet security settings are set to their recommended levels.

User Account Control On

UAC will always notify and wait for a response.

 [Change settings](#)

Network Access Protection Off

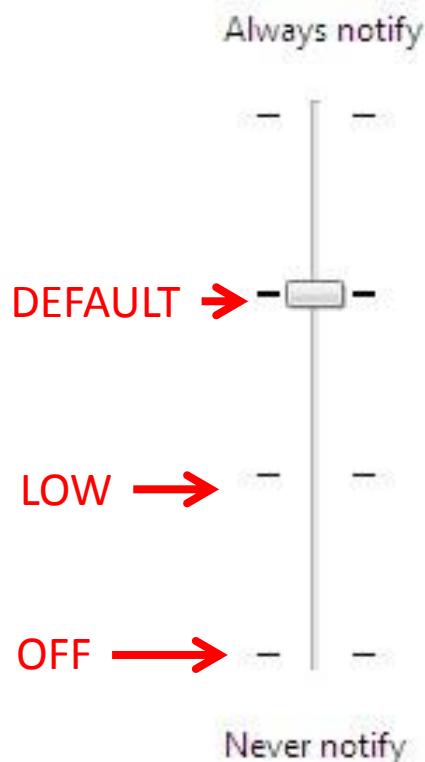
Network Access Protection Agent service is not running

[What is Network Access Protection?](#)




## Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.  
[Tell me more about User Account Control settings](#)



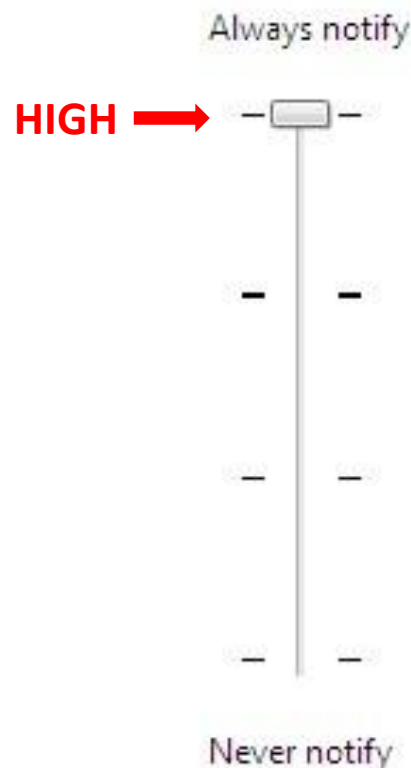
### Default - Notify me only when programs try to make changes to my computer

- Don't notify me when I make changes to Windows settings

 Recommended if you use familiar programs and visit familiar websites.


## Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer. [Tell me more about User Account Control settings](#)



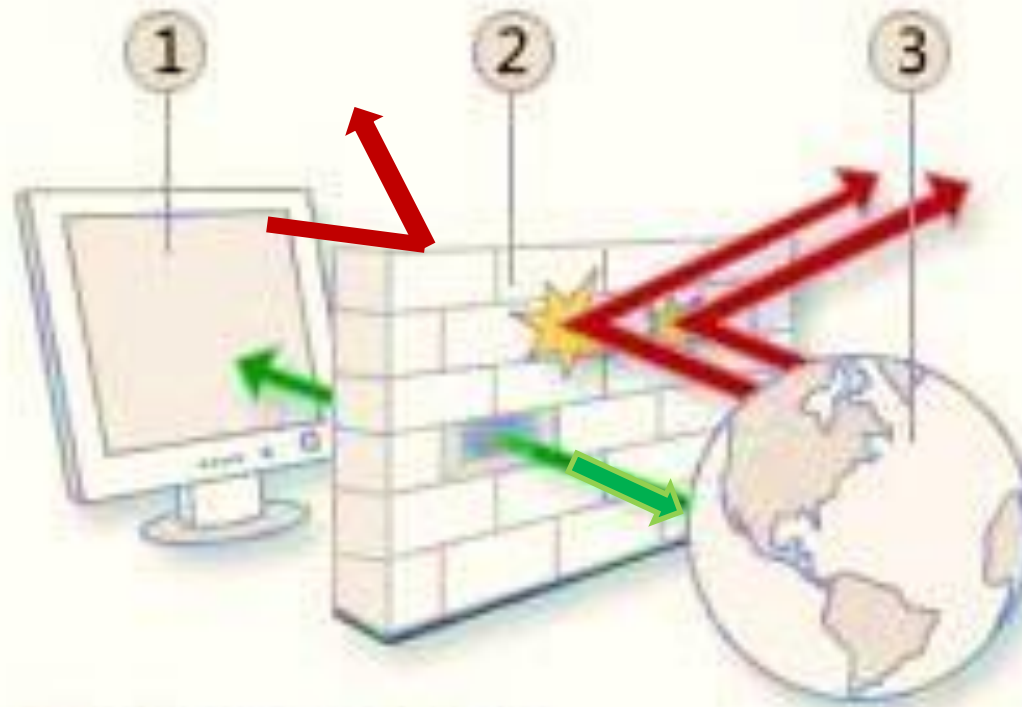
### Always notify me when:

- Programs try to install software or make changes to my computer
- I make changes to Windows settings

 Recommended if you routinely install new software and visit unfamiliar websites.

# Control Panel Windows Firewall

Zone Alarm (a third party firewall)  
used to be the preferred default



① Your computer

② Your firewall


③ The Internet


The Firewall limits the type of internet traffic That can enter or leave your PC


Control Panel Home

Allow a program or feature through Windows Firewall

 Change notification settings

 Turn Windows Firewall on or off

 Restore defaults

 Advanced settings

Troubleshoot my network

## Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

[How does a firewall help protect my computer?](#)

[What are network locations?](#)

  Home or work (private) networks	Connected 
Networks at home or work where you know and trust the people and devices on the network	
Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	 Network
Notification state:	Notify me when Windows Firewall blocks a new program
  Public networks	Not Connected 

# Anti Virus and Anti Malware

# Top 10 Anti Virus / Anti Malware program assessment 2013

## By AV Comparatives.ORG

Kaspersky Labs	A+ ( overall top score)	\$NZ 40
Bit Defender	A+	Free version
Avira	A+	Free version
Fortinet	A+	(for complex networks)
ESET	A+	\$NZ 85
Avast	A+	Free version
Microsoft Security	A	Free
Microsoft Defender	A	Free
F-Screen	A	\$NZ 60
BullGuard	A	\$NZ 50



Microsoft Security Essentials

Microsoft Defender

These two names are essentially the same product.  
Defender comes with Windows 8  
Security Essentials has to be downloaded separately

These are easy to set up and use  
Examples follow in the next 5 slides

PC status: Protected

- Home
- Update
- History
- Settings

Help



Your PC is being monitored and protected.

- Real-time protection: On
- Virus and spyware definitions: Up to date

Scan options:

- Quick
- Full
- Custom

Scan now



Scan details

Scheduled scan: Sunday around 2:00 a.m. (Quick scan) | Change my scan schedule

Last scan: 20/01/2014 at 3:38 p.m. (Quick scan)

**PC status: Protected**

Home

Update

History

Settings

Help ▾

**Virus and spyware definitions:** Up to date

Your virus and spyware definitions are automatically updated to help protect your PC.

Definitions created on:	31/01/2014 at 5:23 p.m.
Definitions last updated:	31/01/2014 at 8:41 p.m.
Virus definition version:	1.165.3030.0
Spyware definition version:	1.165.3030.0

Update

**Did you know?**

Virus, spyware, and other malware definitions are files that are used to identify malicious or potentially unwanted software on your PC. These definitions are updated automatically, but you can also click Update to get the latest versions whenever you want.

PC status: Protected

- Home
- Update
- History
- Settings

? Help ▾

View the items that were detected as potentially harmful and the actions that you took on them:

**Quarantined items**

Items that were prevented from running but not removed from your PC.

Allowed items

Items that you've allowed to run on your PC.

All detected items

Items that were detected on your PC.

Detected item	Alert level	Date

- Remove all
- Remove
- Restore

PC status: Protected

Home

Update

History

Settings

Help

Scheduled scan

Default actions

Real-time protection

Excluded files and locations

Excluded file types

Excluded processes

Advanced

MAPS

Turn on real-time protection (recommended)

Real-time protection alerts you whenever malicious or potentially unwanted software attempts to install itself or run on your PC.

Save changes

Cancel

PC status: Potentially unprotected

Home

Update

History

Settings

Help



You haven't run a scan on your PC for a while. This could put your PC at risk.

- Real-time protection: **On**
- Virus and spyware definitions: **Up to date**

Scan options:

- Quick
- Full
- Custom

Scan now

Scan now



Scan details

Scheduled scan: **Sunday around 2:00 a.m. (Quick scan)** | [Change my scan schedule](#)

Last scan: 20/01/2014 at 3:38 p.m. (Quick scan)

## **The final defence against Cryptolocker is “recovery”.**

A) Regularly make off line backup copies of important documents  
They may be a little out of date but that is usually a minor issue compared to loosing the whole file.

OR

B) The most secure option is a backup method called imaging or cloning.  
A complete replica of your total hard drive is created for the Operating System, the Application Programs and your Data Files  
( it is usually compressed to save backup disk space)

This not only protects you against Cryptolocker type attacks but can quickly replicate a Hard Drive if you have a major hardware failure.

**Paragon Backup & Recovery Free 2013**  
**CloneZilla Live**

Are two options