Over Peover Online   How to….

Protect your data

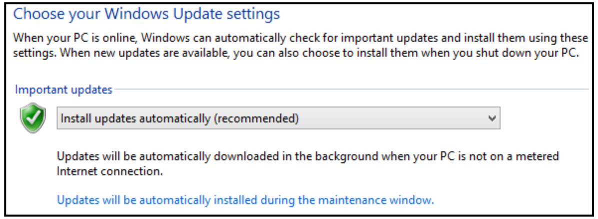
Securing your home network

- Intruders can break into your home network and steal your data unless you keep them out.
- Your router will probably broadcast its name (SSID) so your wireless devices can find it to connect to. However, this is public outside of your house too. You should always use a strong password and ensure your router is using WPA2 encryption. If you want, you can disable the router broadcasting its name in the router settings once you have set up all your wireless devices. Also ensure that the router firewall is on (this is the normal default state).
- If you suspect someone knows the password then change it.

Securing your computer

- □ Ensure you have a currently supported operating system (OS-X, Windows or Linux) and software
- □ Ensure that your operating system is set to receive security updates automatically
- □ Ensure your PC firewall is enabled
- □ Ensure your PC is protected with a user account log-in and password to prevent visitors accessing your data
- □ Ensure you have up to date anti-virus software
- □ Don’t use public WiFi hotspots to send personal information unless it is a secure connection (check that the address starts https:\\ and the padlock symbol is present)

Support for Windows XP and Office 2003 Ends April 8th 2014



Choose your Windows Update settings

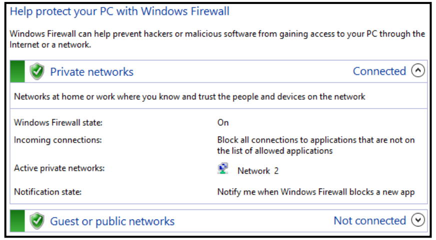
When your PC is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also choose to install them when you shut down your PC.

Important updates

Install updates automatically (recommended)

Updates will be automatically downloaded in the background when your PC is not on a metered Internet connection.

Updates will be automatically installed during the maintenance window.



Help protect your PC with Windows Firewall

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

Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

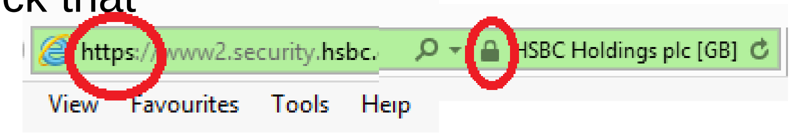
Windows Firewall state: On

Incoming connections: Block all connections to applications that are not on the list of allowed applications

Active private networks: Network 2

Notification state: Notify me when Windows Firewall blocks a new app

Guest or public networks — Not connected



https://www2.security.hsbc.

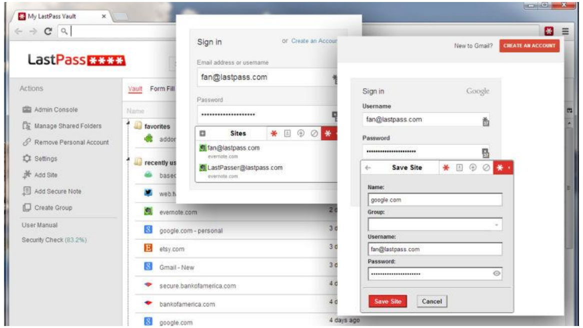
HSBC Holdings plc [GB]

Passwords

- If you do a lot of online shopping you will be suffering password fatigue. Research shows that 55% of internet users use the same password for each website which is great news for criminals but bad for your security.
- Remembering so many can be impossible but here are some suggestions:
  - Don’t use easily guessed names or numbers such as pet names or dates of birth
  - You can used a passphrase instead and take the first letter of each word plus some numbers and use a mix of upper and lower case letters (I want to get my Golf Handicap to less than 18 gives IwtgmGH2<18)
  - You can insert some element of the website address into the password so each website password is different but don’t use the whole name. Using the example above for Amazon and inserting the password between the first and last letters of Amazon gives AIwtgmGH2<18n.
  - Try to use a symbol as well such as the “less than” < symbol above or #£$%&”! etc.

Passwords continued

- If you follow the guidelines on the previous slide you will be better than most internet users.
- Another option is to use a Password Manager.
- These are software programs that generate random strong passwords and store them in an encrypted form. To access them the Password Manager is itself password protected but at least that is only one password to remember now!
- Some work and sync across multiple platforms such as Windows, iOS, Android etc. and some are even free.



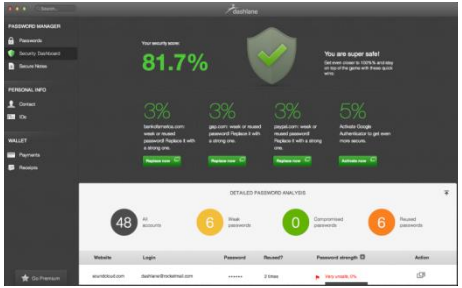
Email address or username: fan@lastpass.com

Sites: fan@lastpass.com, LastPasser@lastpass.com

Username: fan@lastpass.com

Name: google.com

Username: fan@lastpass.com



You are super safe! Get even closer to 100% and stay on top of the game with these quick wins.

bankofamerica.com: weak or reused password! Replace it with a strong one.

gap.com: weak or reused password! Replace it with a strong one.

paypal.com: weak or reused password! Replace it with a strong one.

Activate Google Authenticator to get even more secure.

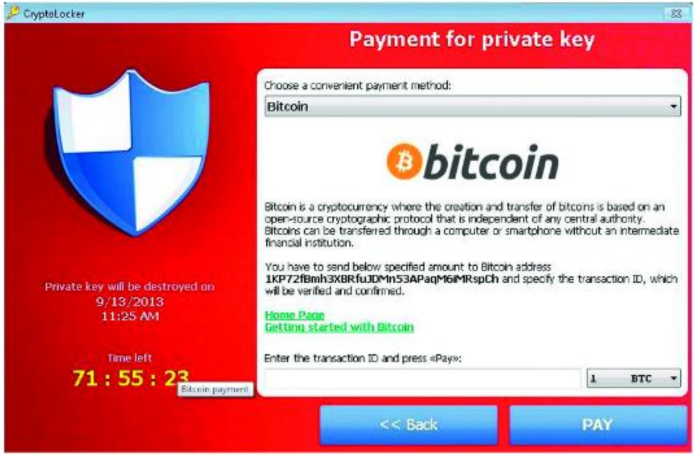
Website	Login	Password	Reused?	Password strength	Action
soundcloud.com	dashlane@rocketmail.com	•••••••	2 times	Very unsafe, 0%	

Viruses, worms & trojan horses

- □ A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves.
- □ A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.
- □ A trojan horse is a program that claims to rid your computer of viruses or speed it up but instead introduces viruses onto your computer. Beware of downloading programs unless you trust the site and generally go to the makers site to get it if you can.
- □ Protect yourself by using anti-virus software and ensuring it is up-to-date. There are subscription ones available but also good free ones like AVG.
- □ However, prevention is better than cure. Viruses often come via email attachments so **DO NOT** open an attachment unless you recognise who it is from.

Ransomware

- One special type of virus is named Ransomware because, as its name suggests, it locks the computer completely and extorts a ransom to unlock it again.
- One case was the Cryptolocker virus that demanded payment of one bitcoin (an internet currency purchased with real money:
  1 bitcoin ≈ £280)
- This was particularly difficult to remove and re-installing the entire operating system was necessary in some cases with the loss of all data files which is where regular back-ups become so important.



Choose a convenient payment method: Bitcoin

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send below specified amount to Bitcoin address **1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh** and specify the transaction ID, which will be verified and confirmed.

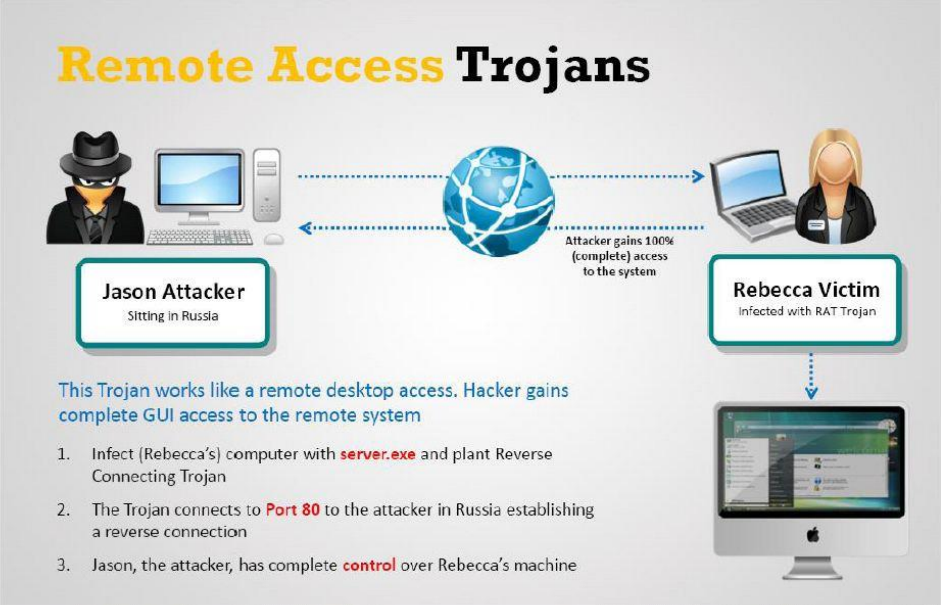
Enter the transaction ID and press «Pay»: 1 BTC

Private key will be destroyed on
9/13/2013
11:25 AM

Time left
71 : 55 : 23

RAT’s (Remote Access Trojan)

- □ RAT’s are Trojan Horse programs that give remote access control of your computer to a criminal.
- □ They can then spy on your activity online, see what you are typing, can alter files or delete them, format your hard drive or record you via a webcam if you have one.
- □ The information can then be used to access your bank account, make purchases in your name or blackmail you.



Remote Access Trojans

This Trojan works like a remote desktop access. Hacker gains complete GUI access to the remote system

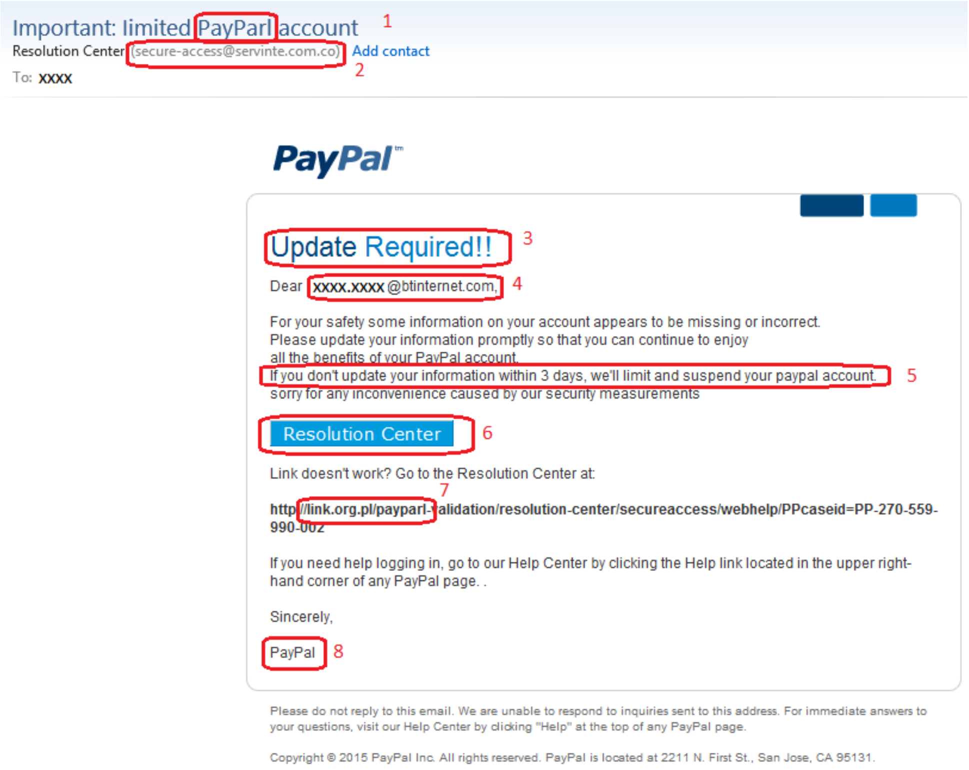
1. Infect (Rebecca’s) computer with **server.exe** and plant Reverse Connecting Trojan
2. The Trojan connects to **Port 80** to the attacker in Russia establishing a reverse connection
3. Jason, the attacker, has complete **control** over Rebecca’s machine

Phishing emails

- **Phishing** is typically carried out by email and often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
- Phishing emails can sometimes be hard to spot. Here are some signs that an email may be phishing:
  - It is addressed “Dear customer” or “Dear <email address>” not to a named individual.
  - It will engender a sense of worry or panic often with a need to act immediately such as “your account has been blocked”.
  - It will contain a hyperlink to the fake website such as “click here to log in”. Hover your mouse over it and see if it starts with the company website address.
  - The logo may be poor quality
  - The grammar or spelling may be incorrect or use US spelling
  - You’re asked to send money or promised large sums by making contact

Example phishing email

1. Incorrect spelling of PayPal
2. Does not originate from PayPal
3. Exclamation marks would not be in a genuine email
4. Addressed to Dear <email address>
5. Threat accompanied with urgency
6. Hyperlink to fake website
7. Hyperlink does not start PayPal.co.uk but is a Polish website (.org.pl)
8. Not from a person also would be “Yours Sincerely” if from the UK and usually accompanied with department or job title.



Important: limited PayParl account

Resolution Center (secure-access@servinte.com.co) Add contact

To: xxxx

PayPal™

Update Required!!

Dear xxxx.xxxx@btinternet.com,

For your safety some information on your account appears to be missing or incorrect.
Please update your information promptly so that you can continue to enjoy
all the benefits of your PayPal account.
If you don't update your information within 3 days, we'll limit and suspend your paypal account.
sorry for any inconvenience caused by our security measurements

Resolution Center

Link doesn't work? Go to the Resolution Center at:

http://link.org.pl/payparl-validation/resolution-center/secureaccess/webhelp/PPcaseid=PP-270-559-990-002

If you need help logging in, go to our Help Center by clicking the Help link located in the upper right-hand corner of any PayPal page. .

Sincerely,

PayPal

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" at the top of any PayPal page.

Copyright © 2015 PayPal Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.

What to do with a phishing email

- **DO NOT** under any circumstances click on any hyperlinks in the email
- **DO NOT** send money anywhere
- **DO NOT** enter any username, account details, password or PIN
- **DO NOT** panic or worry whatever the content says. Genuine organisations do not send unsolicited emails to frighten the public or their customers
- If it pretends to be from a genuine organisation such as a bank, forward the email onto them if they have a phishing inbox (e.g. phishing@hsbc.co.uk). They can then take action against the perpetrators otherwise delete it. **DO NOT** forward it on to anyone else.
- If you are unsure if it is genuine or a phishing email then phone the company and ask them but **DO NOT** use any phone number in the email. **DO NO**T use any hyperlink in the email but instead get the company phone number through Google search.

Vishing

- **Vishing** is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.
- The latest trick is to ask the victim to hang up and dial the number on the back of their bank card, however the scammers don’t hang up and pretend to answer the phone as if genuine fooling the victim into thinking they have got through to their bank. Always wait 5 minutes from hanging up for the line to clear before dialling or use a mobile phone.
- Your bank will never ask you for your PIN or online banking password over the phone.
- **NEVER** disclose your password to anyone no matter how genuine they may sound. If anyone asks for it, it is a sure sign they aren’t genuine. Hang up **IMMEDIATELY.**
- **NEVER** transfer money online on someone else’s instruction or advice.

Social networking

- If you use social networks to share information about yourself make sure you know who you are sharing it with
- Ensure your privacy settings are set correctly and don’t make public information that will help criminals. For example:
  - If you are in a sensitive job don’t advertise the fact and make yourself vulnerable to blackmail
  - If you are going away on that dream holiday don’t advertise that you will be away and the house will be empty
- Posting comments on social media is still “publishing” and commenting on live court cases could render you in contempt of court and liable to prosecution.

Protecting mobile devices

- Mobile devices such as laptops, tablets, smartphones and memory sticks are easily lost, stolen or broken if dropped. You may lose your data and that data may also fall into the wrong hands.
- Ensure your mobile device is locked with a good password or fingerprint. Swiping a pattern is much less secure.
- Do not leave them unattended when travelling
- Back up any important data regularly

- If your smartphone or tablet breaks and needs to be sent for repair back up all data and apps first then reset it back to factory condition before sending it off. When it comes back, restore your data and apps from the back up.

Backup your data

- A key activity in using computers is to always back up your data.
- As people use many different devices these days this becomes more complex.
- Let’s look at some possibilities and their advantages and disadvantages

SugarSync
iCloud
Microsoft SkyDrive
Dropbox

Backup your data cont’d

Method	Advantages	Disadvantages	Comment
Use CD’s or DVD’s	Cheap @ 20p per disc Backup easily stored in a different location	Capacity limited to 4.7GB per disc Each backup needs to write all the data each time	Only practical for small backups Not suitable for mobile devices
Use external hard disc drive	Sizes up to 6TB Supports incremental backups	Difficult to back up multiple devices.	Cost from £30 (500GB) to £200 (6TB) Some new ones use WiFi

Backup your data cont’d

Method	Advantages	Disadvantages	Comment
Use extra internal hard disk drive	Faster backups than external drive	Needs some hardware knowledge	Easy to schedule routine backups. Only suitable for desktop PC’s
Use cloud storage	Infinite capacity Supports multiple devices Data available anywhere there is internet	Puts your data in someone else’s hands which is a greater target for hackers	An amount of free storage then monthly subscription for larger amounts

Backup your data cont’d

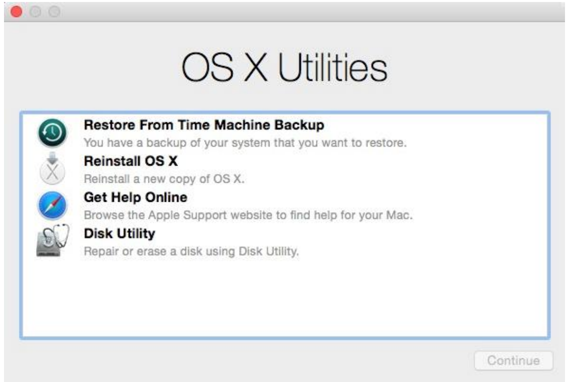
- For smartphones and tablets it is normal to back up your apps and data to a computer.
- The manufacturers of the device often have programs on their websites to do this. Apple uses iTunes or iCloud, Samsung uses Smart Switch, HTC uses Sync Manager, Nokia uses Nokia Suite.
- Some phones can back up data to cloud storage directly but may not back up downloaded apps or individual settings. Refer to your phone or tablet manufacturers website for more detail.
- Some backups create a new backup entirely rather than overwrite previous backups. This can consume large quantities of hard disc space if performed regularly. In this case you may need to delete old backups manually.

Disposing of old devices

- Computer devices have a relatively short life and the time will come when it is necessary to dispose or recycle them. However, your devices will likely contain a lot of personal data that needs to be protected.
- First step is to transfer all the data you want to keep onto another device
- Smartphones and tablets – Remove any microSD and SIM cards and reset the device back to factory condition (usually found in the settings menu)
- Windows® laptops and desktop PC’s need to have their hard discs wiped or destroyed. Formatting the disc **DOES NOT** destroy the data. This applies to USB sticks, SD cards and camera Compactflash cards as well.
  - To destroy a hard disk permanently remove it and smash it with a sledgehammer or send it to a secure destruction service for melting down (this is what some government agencies do).
  - To wipe data from a hard disc/USB stick/SD card etc without physically destroying it, it needs to be written over the surface with random zero’s and one’s at least 3 times and preferably more. You can download any number of programs to do this and preferably use one that can be booted from a USB stick or CD so it can wipe the entire disc including the operating system. If you want to reinstall the operating system afterwards make sure you have bootable media and the product key. If your computer didn’t come with Windows installation media you can download it from Microsoft. If you don’t know your product key look for a sticker on the machine or try running Belarc Advisor.

Disposing of old devices cont’d

- Apple Macs can have their discs wiped by using a built in utility.
  - Click the Apple menu at the top of your screen and select Restart. After your Mac restarts and when you see a grey screen, press and hold down the Command (⌘) and R keys at the same time. You’ll enter OS X Recovery and the first thing you’ll see is a “choose your language” screen. Select English and you will then get 4 options.
  - Select Disk Utility and select your Mac OS X start-up disk. Click the Erase tab and use the options here to erase the entire disk. All your files, including the Mac OS X operating system itself, will be wiped away. If you have a Mac with a mechanical hard drive, be sure to click the Security Options button.
  - Restart the machine and repeat step 1 to enter OS x Recovery again. From the OS X Recovery menu, select the option Reinstall OS X



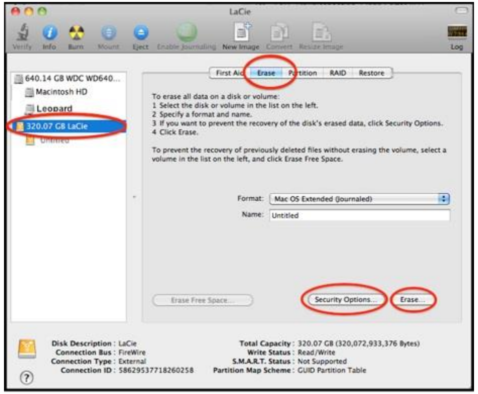
OS X Utilities

Restore From Time Machine Backup
You have a backup of your system that you want to restore.

Reinstall OS X
Reinstall a new copy of OS X.

Get Help Online
Browse the Apple Support website to find help for your Mac.

Disk Utility
Repair or erase a disk using Disk Utility.



To erase all data on a disk or volume:
1 Select the disk or volume in the list on the left.
2 Specify a format and name.
3 If you want to prevent the recovery of the disk’s erased data, click Security Options.
4 Click Erase.

To prevent the recovery of previously deleted files without erasing the volume, select a volume in the list on the left, and click Erase Free Space.

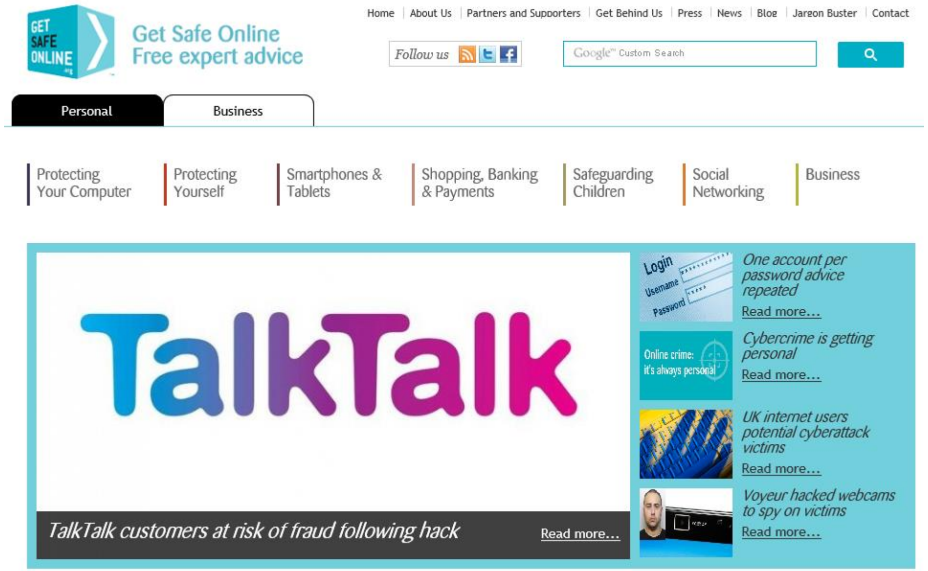
Format: Mac OS Extended (Journaled)
Name: Untitled

Disk Description : LaCie
Connection Bus : FireWire
Connection Type : External
Connection ID : 58629537718260258

Total Capacity : 320.07 GB (320,072,933,376 Bytes)
Write Status : Read/Write
S.M.A.R.T. Status : Not Supported
Partition Map Scheme : GUID Partition Table

Further information

- ◻ This guide just scratches the surface of a very large subject and there are much more detailed guides available.
- ◻ One of the best websites is www.getsafeonline.org which is a free impartial advice site and is a public / private sector partnership supported by HM Government and leading organisations in banking, retail, internet security and other sectors.



TalkTalk customers at risk of fraud following hack Read more…

One account per password advice repeated Read more…

Cybercrime is getting personal Read more…

UK internet users potential cyberattack victims Read more…

Voyeur hacked webcams to spy on victims Read more…