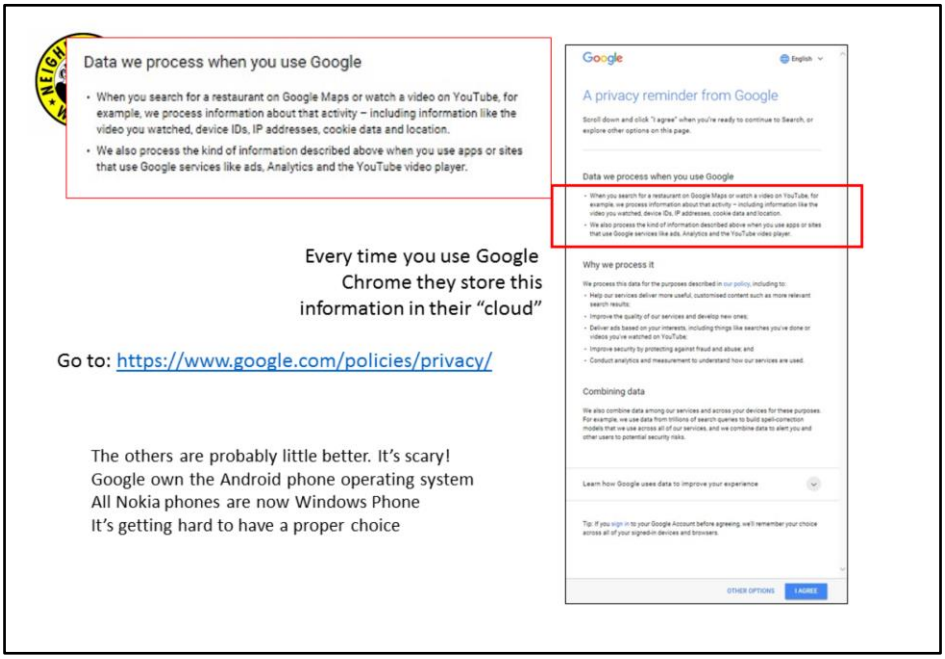
How to stop making it easy for criminals

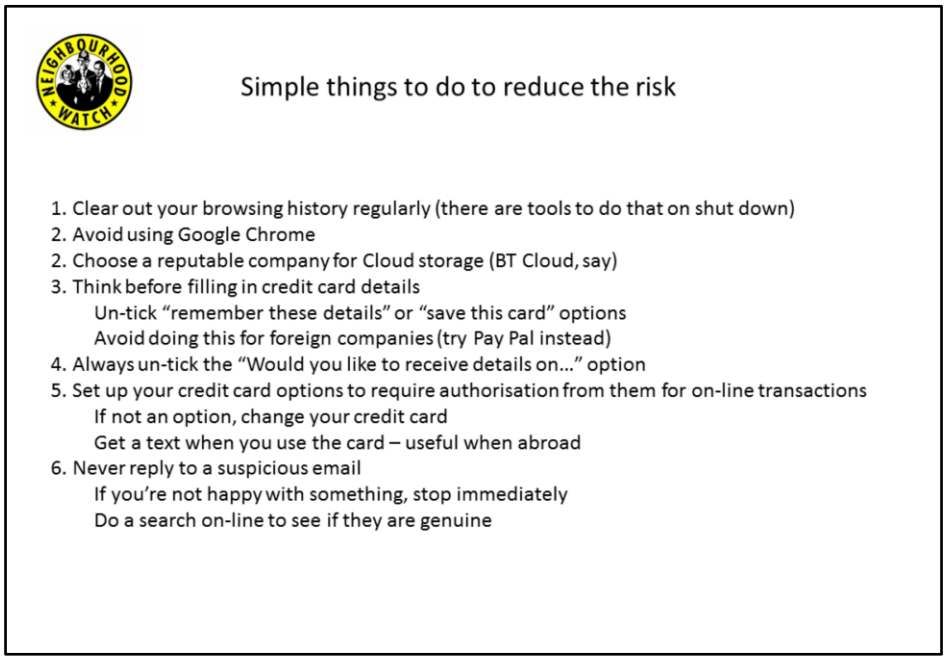
It's so easy to do things on your PCs, tablet and phone.

But what happens to all that information and data?

Modern IT systems communicate with each other via large networks that can manage an enormous amount of data. Until recently, the networks would all be dedicated links between various datacentres, offices and the public. The knowledge of who had access to the data between A and B was easy to track. The modern way of designing computer systems is to do away with that dedicated link and tight control and to put the supplier systems in datacentres that could be anywhere. This is the concept of "the cloud". Your data is "up there somewhere". Your data disappears into "the cloud" and you do not know who has it and what they are doing with it. Of course, it's nowhere as simple as that and there are very tight controls everywhere, but it does add an element of doubt into the security of the data. The industry makes every effort to ensure your data is secure, but it only requires one small error by one person for things to go wrong.



To illustrate what could be happening to your private information, just look at Google's published privacy statement. They are saying that they hold information about you, what you have searched for, where from and the address of your PC or laptop (it's called the IP address). That marketing information goes in "The Cloud" If you have a Google account you may do searches on your PC and then retrieve the history of those searches from your iPhone a week later from somewhere completely different. Your account information is held centrally, by Google. Do you trust them to never let that information get known to anyone else? Do you?
Why not avoid the risk and make sure you do some simple things every time you use your computer, laptop, tabled, phone, etc. The next slide has some general advice.

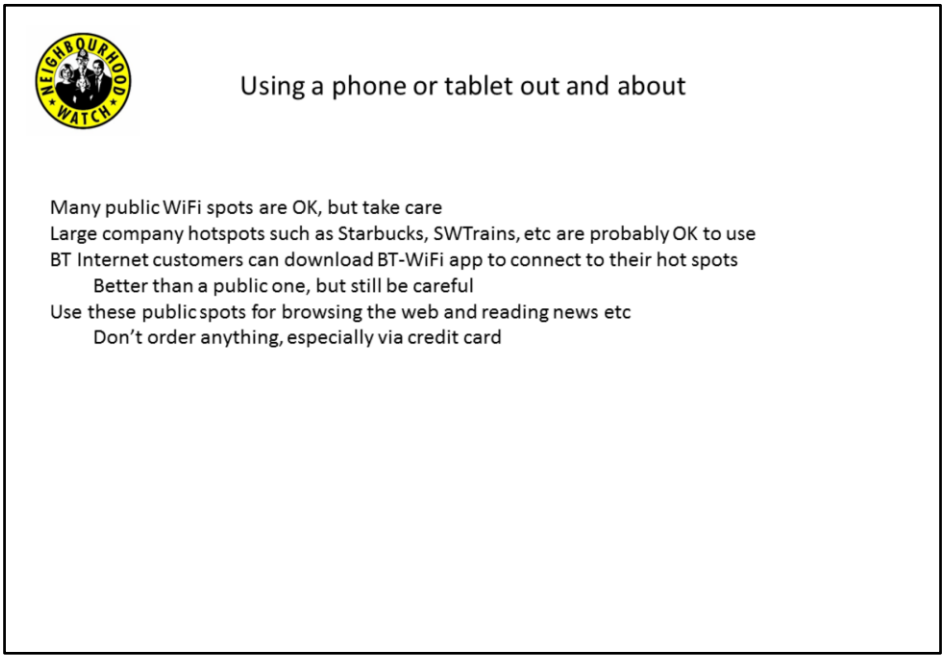


1. Clear out your internet search history, your temporary internet files etc, every time you close down. There are tools out there to do that for you and some are free. The better ones cost a small amount as a one-off purchase charge. CCleaner and PC Cleaner are two examples but there are others. Some web browsers have these settings.
2. Google Chrome is definitely Big Brother (and they don't like paying their UK taxes!). Avoid. Try others. Mozilla Firefox is much more friendly.
3. Storing your personal data on "the cloud" is not a problem, but choose a company you trust. BT's Cloud service seems as good as any. Buy from the right company, not because the price is cheapest. Also, don't forget that the data is only available when you are on-line. If you are in a bad signal area you'll not be able to connect and so not be able to access that data.
4. When you buy something online, say, you have to option to unsubscribe to follow-up marketing information. The less reputable companies make you tick a box to not receive following up emails. Always make sure you unsubscribe, unless you really do want to receive marketing emails.
5. Most banks now have an option that requires them to automatically vet the company you are buying from and ask for an on-line authorisation from you if there is any doubt. Reputable retailers will be registered and not need their sales

authorised by you on line. If your credit card supplier does not offer this option, change your credit card supplier. When abroad, most credit card companies offer a facility to text you when a transaction is made. But be careful to check whether your mobile phone company will charge you a lot to receive the text.

6. If you get an email that is suspicious, “hard” delete it. <CTRL>+ delete actually deletes it from your mailbox and doesn’t keep it in a “deleted email” mailbox. Never open a link or attachment in a suspicious email. Before deleting you may want to do a search on their email address to see whether it is a scam or not. Some reputable organisations stupidly send emails out from email addresses that look fake (HMRC do, for example).

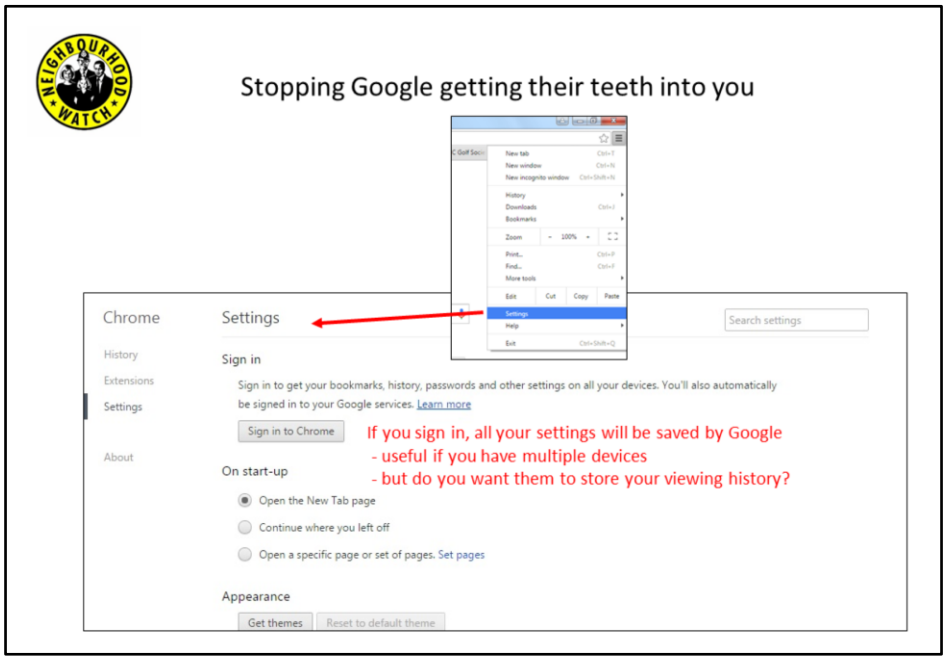
Think who you are dealing with. Would you trust John Lewis Partnership/Waitrose? Of course you would. Would you trust a company called “CheapestFlights.com”? I hope your answer is “no”.



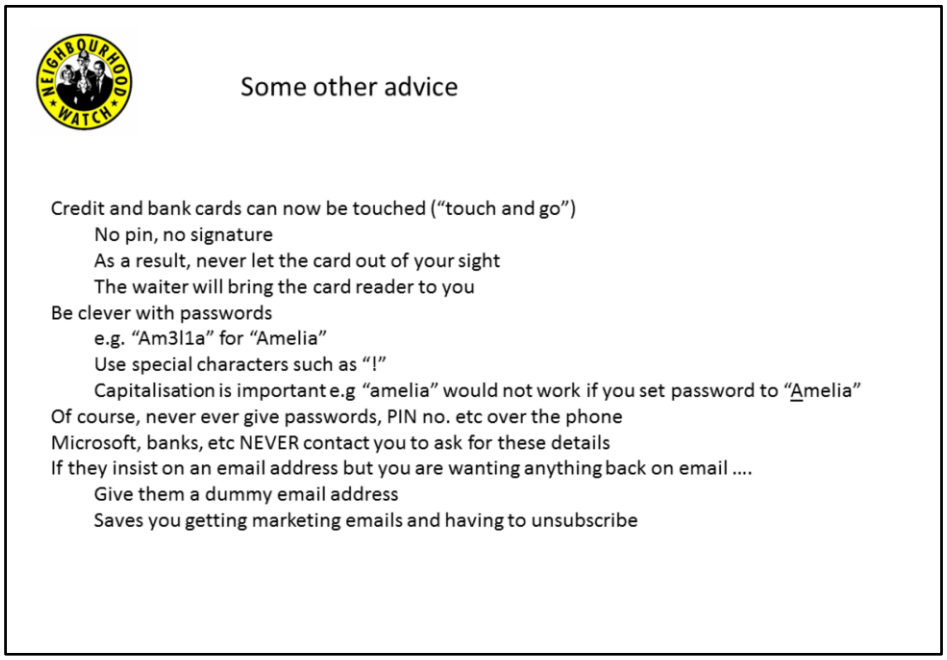
We can now access the world from most places. For example, most café chains have free WiFi connections. As a general rule, free WiFi from reputable companies is going to be OK as their reputation is at stake if someone thinks they are being hacked whilst sitting in their café (say).

If you are a BTInternet customer you can get access to BT hot-spots using your BT account logon. There's a phone App that will do this for you.

No matter who the public WiFi supplier is, avoid doing financial transactions across such links – wait till you get home. It's better to be safe than sorry.

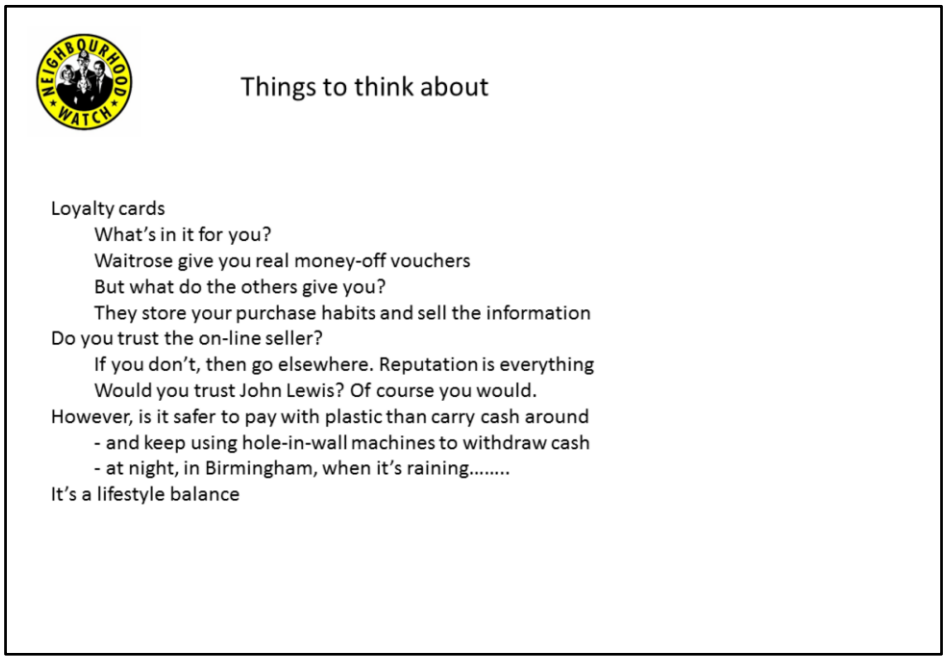


I mentioned about Google "Big Brother" above. There are ways to reduce their hold on you. The easiest thing to do is change the default Chrome settings on you PC to NOT sign in automatically to your Google account. By default, the software is loaded with auto-sign in. This slide shows how to set that off. By doing this your search details, etc, will not get onto the Cloud because you are not signed into the account.



We are becoming a cashless society. "Touch and Go" is useful for small purchases – no need to put the pin in. Millions do it. But never let the card out of your sight. If a waiter takes the card away they can easily brush it against their card reader and £20, or more, comes out your account and there's nothing you can do about it.

It's an old bit of advice, but be careful with passwords. Be clever with them as in the examples in this slide. Never give them to anyone, particularly over the phone. Have a minimum of 3 passwords you use regularly (but no more than 3 in case none are the right one and you lock out your account).
If you have to give an email when you buy something from a supplier, but you don't want any email back, stick a dummy email address in (make sure it's an obvious dummy and not some unfortunate other person's email address). Do they insist on a mobile number but you don't want to give it (or do not own a mobile)? Put a fake number in. All 077009 numbers are fakes. So put in, say, 07700912345.



Why have a loyalty card? What's in it for you? Very little, I suspect. But there's a great deal in it for the supplier. They store your purchase history and use it to improve their sales. They bombard you with marketing emails. They sell the information to other companies. For what? You may get 10p every few months in return. Some cards may be worth having, such as Waitrose, as you sometimes get real money-off vouchers that are worth having. Most retaillers are nowhere near as generous as this.

But all of this is a balance. Do you avoid credit cards and use cash all the time? Is it riskier to keep using cash machines, or carrying a fat wallet?

Be careful, it's a nasty world out there.