Jisc evidence to Culture, Media and Sport Committee enquiry into Cyber security: Protection of Personal Data Online

Jisc is the UK's expert body for digital technology and digital resources in higher education, further education and research. Since its foundation in the early 1990s, Jisc has played a pivotal role in the adoption of information technology by UK universities and colleges, supporting them to improve learning, teaching, the student experience and institutional efficiency, as well as enabling more powerful research. Jisc operates the Janet computer network: connecting universities, colleges and research organisations to each other and to the global Internet. We provide advice and services to those customers on appropriate security measures for their on-line activities; our incident response team – Janet CSIRT – coordinates the response to attacks that may affect the network and its customers.

The following are our views on some of the areas mentioned in the consultation paper

The nature of the cyber-attacks on TalkTalk's website and TalkTalk's response to the latest incident

At the time of preparing this response there is very little verifiable information in the public domain about the nature of the attack on TalkTalk's website. Our experience has been that that premature speculation about the causes of cyber-attacks has the potential to distract from, and cause damage to, efforts to investigate and learn from them.

The robustness of measures that telecoms and internet service providers are putting in place to maintain the security of their customers' personal data and the level of investment being made to ensure their systems remain secure and anticipate future threats

Taking into account our response to the previous question, there is very little public domain information to indicate that the attack on TalkTalk is representative of the state of cyber security and preparedness within the telecoms and ISP industries.

However we note that the vulnerabilities (such as "SQL injection") most often exploited to create this kind of breach of customer data are not limited to telecoms and internet service providers. Any organisation participating in e-commerce, in any industry, should be taking appropriate and continuing measures to ensure their systems are not vulnerable to similar attacks.

The nature, role and importance of encryption in protecting personal data

Encryption is one of a number of important tools in protecting personal data. It can be used for at least two different roles:

1. protecting passwords, personal and other sensitive information as it is transmitted across communication networks;
2. protecting stored information against physical theft.

When sending personal or other sensitive data across a communications network, encryption should be used to protect it against those who may have access to the intervening network. For example when using wireless networks all communications can be read by anyone within

radio range (typically 100 metres or more). Encryption, such as a Virtual Private Network, should be used to prevent such listeners obtaining transmitted information in an intelligible form. The scope for listening-in to a physical network is less, but any website that may transmit or receive confidential data should offer an encrypted (HTTPS) connection as a default. Despite recommendations from the Information Commissioner this is still far from universal practice.

Setting up encrypted communications is generally straightforward. But, like any online service, software needs to be kept up to date to address newly-discovered technical weaknesses. For encryption software, regular updates are also required to keep up with developments in cryptography. Settings that may have been considered secure in the past may no longer be so due to developments in mathematics and computing power; these should normally be updated. If it is essential to continue to support all customers, no matter how out of date and insecure their computers may be, then obsolete settings should be limited to separate systems where the increased risk can be managed without affecting others.

When information is stored on a computer, encryption can protect it if the computer is stolen or otherwise falls into the wrong hands. This is most important for portable devices that can easily be lost or stolen - the Information Commissioner expects personal data to be encrypted if stored on laptops or portable disk drives. Provided appropriate software is used (this is built in to most current operating systems) and a strong password used by the legitimate user to gain access, this should prevent a casual thief obtaining access to the information.

However encryption is much less effective in protecting information against attacks (such as SQL injection) via the applications used by those with legitimate access. When accessing any on-line service, sensitive information should be encrypted when stored on the host computer and when transmitted over the network to the user. But for the user to be able to read the information, it must be converted to unencrypted form. This means that an attacker who can gain control either of the user's computer or of the web application that provides the on-line service will also be able to read and record the information in unencrypted form.

Such attacks on applications are increasingly common. To protect against them organisations need to ensure that applications and software are regularly updated and tested to ensure they contain no known vulnerabilities. The impact of a successful attack can be reduced by separating the information the on-line service requires from other information that the organisation may hold about the customer. If an application cannot access unnecessary information then it will be much harder for an attacker to misuse it.