5th October 2016

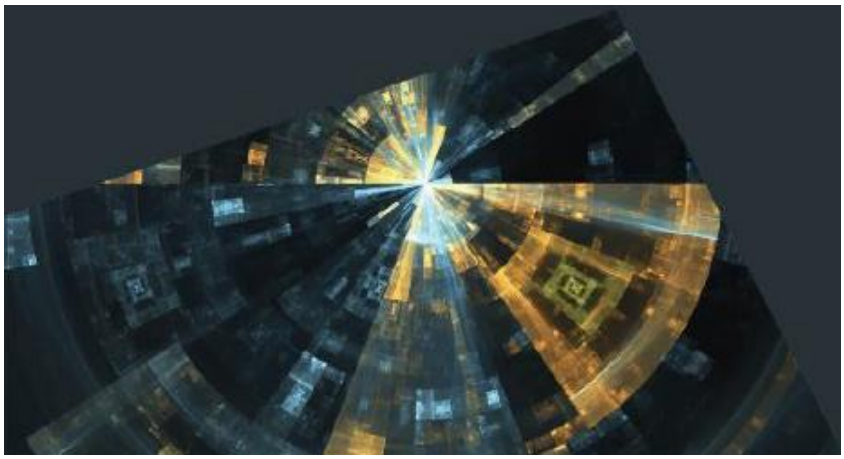
Cyber Matters

Your essential guide

In this issue:

01704 542 420
info@p-ccomms.com

FBI Releases Ransomware Advice



After a number of recent media reports in which an FBI agent was quoted saying that the agency condones paying ransomware demands, a new public statement announcement (PSA) was published this week regarding what companies or US citizens should do.
The PSA urges victims of ransomware incidents to report the crimes to federal law enforcement to help the government “gain a more comprehensive view of the current threat and its impact on U.S. victims.” In supporting statements, the FBI advised that they do not support the payment of ransoms as this does not guarantee a victim will regain access to their data. With almost daily reports of new ransomware variants and an ever-growing list of victims, the PSA is a timely reminder of the substantial threat.

- Regularly back up data your important data and verify the integrity of those backups;
- Scrutinise links contained in e-mails and do not open attachments included in unsolicited e-mails;
- Only download software from sites you know and trust (and when possible, verify the integrity of the software through a digital signature prior to execution);
- Ensure application patches for the operating system, software, and firmware are up to date (including Adobe Flash, Java, Web browsers, etc.);
- Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted;
- Disable macro scripts from files transmitted via e-mail;
- Patch all endpoint device operating systems, software, and firmware as vulnerabilities are discovered (e.g. via a centralised patch management system);
- Manage the use of privileged accounts by implementing the principle of least privilege and configure access controls with least privilege in mind;
- Implement application whitelisting

Should I Tape Over My Webcam?

During a talk on national security issues in Washington this week, FBI Director James Comey acknowledged that he places tape over his laptop's webcam to reduce the potential risk of hackers from peering into his private life. Comey, who was widely mocked for previous comments on this matter back in April, highlights an important, but simple, measure that users can take to mitigate the risk of compromise.

It has been widely reported how hackers can install malicious Remote Access Trojans (RATs) onto computers that allows them access to what you type on the keyboard, say near the microphone or do in front of the camera. To protect against this, users should install anti-virus software, use a firewall and not click on any suspicious links in emails, but this additional precaution offers an effective way of bolstering your personal protection.

Jargon Buster: What is RAT?

A remote access Trojan (RAT) is a malware program that incorporates a back door enabling administrative control over a target computer. They are usually downloaded undetected within user-requested programs (i.e. a game or app) or sent as an email attachment. Once a RAT is installed, it can enable a malicious actor to monitor keystrokes, access confidential information, activate the webcam and record video/audio.

61% of UK consumers believe businesses are not doing enough to defend against cyber attacks

A new poll released by F5 Networks shows that half of all consumers would avoid buying from businesses that have suffered a cyber security breach. 3,000 people across the UK, Germany and France were surveyed and revealed that 50% of those questioned would not buy products from, or share data with, any businesses that have been hacked in the past.

UK respondents were shown to be the most judgemental of companies with 61% saying that they don't think businesses are doing enough to protect themselves from hackers (France was 49% and Germany 46%).

Businesses that hold data on European citizens now have an extra incentive to improve their cyber security. The European General Data Protection Regulation (GDPR) will soon come into force which will see businesses face fines of up to 4% of their annual global revenue if they fail to comply. All businesses will also have to report a detected breach within 72 hours.

Be careful what you post

In a case that could well be an early warning of things to come, an 18-year-old woman in Austria is suing her parents for posting embarrassing shots of her as a baby on Facebook.

She says that her parents have shared hundreds of childhood images with their 700 Facebook friends and, having ignored her repeated requests to take them down, she is taking them to court for invasion of privacy.

If she wins the case, her parents could face a fine for their daughter's pain and suffering, as well as potentially being held liable for her legal costs.

This case serves as a timely warning to parents who post prolifically on social media, although parents in France may have more to fear as penalties for those convicted of publicising intimate details of the private lives of others (including children), without first getting their consent, can face up to a year in prison.

Thank you for downloading this guide.

Please feel free to contact us on the details below if you have any questions or comments, or would like advice on any of your own cyber security issues.

01704 542 420
info@p-ccomms.com