CyberGuard Technologies

Proactive Cyber Defence Report

June 2017

On Friday 12 May, a set of global cyber-attacks took place against thousands of organisations including the NHS, and individuals in dozens of countries. These attacks highlighted a number of critical areas in cyber security.

The WannaCry international ransomware attack has highlighted the risks of relying on unpatched software. The scale of the outbreak has been blamed in part on the widespread use of unsupported operating systems such as Windows XP but also machines without the critical MS-17-010 patch. CyberGuard encourages all users to stay up-to-date with security updates and recommends all users to turn on automatic updates.

https://support.microsoft.com/en-gb/help/306525/how-to-configure-and-use-automatic-updates-in-windows

WannaCry ransomware may not have generated the wealth the scammers responsible were hoping for, but since the attack enterprising criminals have been attempting to cash in on the heightened public awareness of WannaCry. Targeting concerns users, scammers have been offering a range of fake 'fixes' and 'support services'.

This type of social engineering is a common methodology for cyber-criminals. Whether viral social media posts, malicious pop-ups or well-crafted phishing campaigns, high profile events such as the WannaCry attack offer cyber-criminals a hook to spread malware or to solicit funds.

It's not only online incidents that criminals seek to take advantage of. Following news of high profile disasters such as hurricane Catrina in 2005, the 2014 Ebola outbreak and the 2015 Nepal earthquake, scammers set up fake charity websites and sent phishing emails in attempts to steal funds donated to victims.

Recent examples of scams piggybacking on the WannaCry incident include:

- Alerts circulating of social media directing users to fake WannaCry patches which deliver malware.
- A phishing email posing as a BT customer service email which informs users they are locked out of their BT account and directs them to a malicious link to obtain a 'security upgrade' to re-establish full access.
- Third party app stores offering 'patches' for mobile users – despite the fact that no mobile operating systems are believed to be vulnerable to WannaCry.

Away from the ransomware attack, CyberGuard is still seeing the use of poor passwords across our customer base. With more and more data breaches in the news it is important that the password you use to access company data is both secure and unique. Did you know that 4 in 10 internet users use the same password for all of their access?

CyberGuard recommends setting a password of at least 12 characters using numbers, special characters and no dictionary words, or alternatively look to implement a to-factor authentication solution.