MEGA

BHS
Information
Technology

MAY 2017, Vol 6

CYBERATTACK – WANNACRY

On Friday 12th of May, the world witnessed the *WannaCry* Ransomware infect over 70, 000 windows systems in the UK's National Health Services.

WannaCry is a malicious software program that exploits a vulnerability in the Microsoft Windows operating system, allowing it to encrypt data on the user's machine and if configured to do so, on accessible network shares.

The infected hosts took control of essential operating theatre equipment, along with MRI scanners and blood refrigerators and according the security experts, this ransomware attack is only the tip of the iceberg.

PHISHING – HOW DOES IT WORK?

A scammer contacts you out of the blue pretending to be from a legitimate business. For example, the scammer may say that the bank or organisation is verifying customer records due to a technical error that wiped out customer data. Or, they may ask you to fill out a customer survey and offer a prize for participating.

PHISHING - WARNING SIGNS

EMAIL:

- The sender email address does not match the web link, or the web link for the service as you know it;
- The email is not addressed to you by name;
- The web link looks different;
- Poor English or spelling mistakes;
- Threats of account de-activation or services being disabled;
- Requests for usernames or passwords. *These will never be requested by email.*

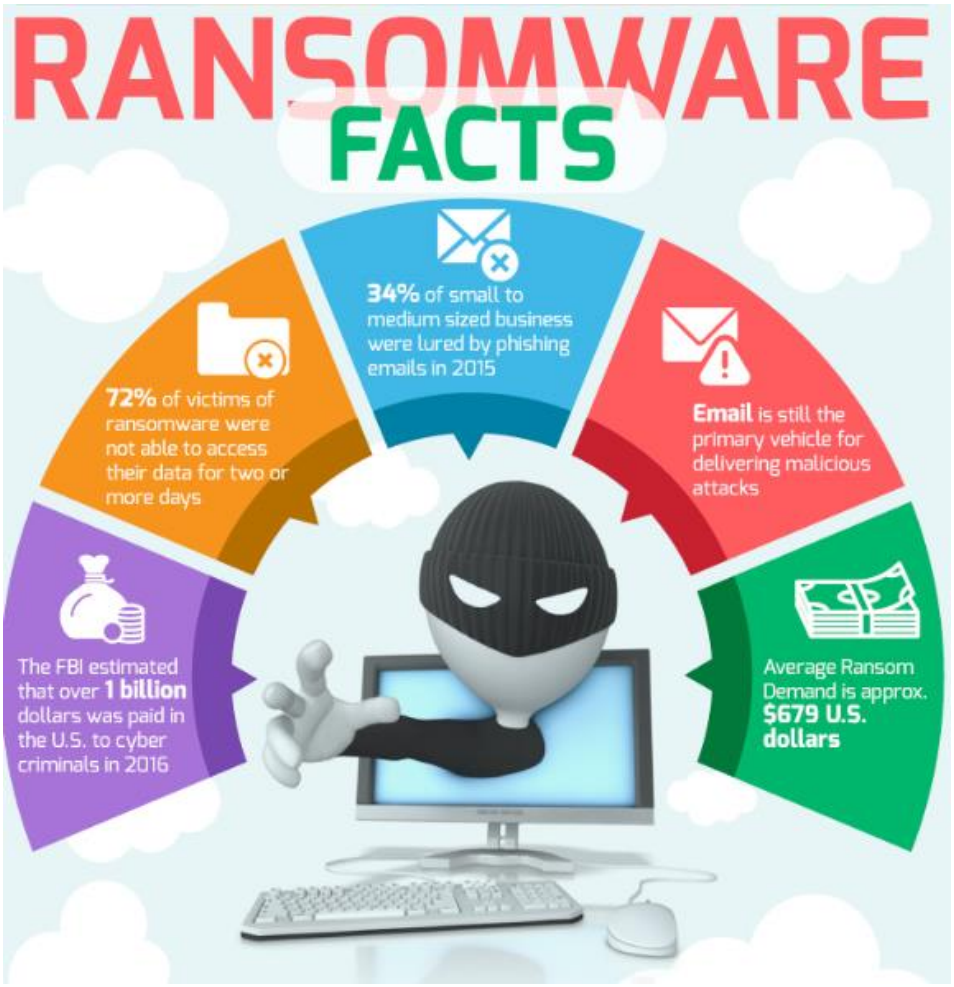
GENERAL

- You notice new icons on your computer screen, or your computer is not as fast as it normally is;
- Offers for help to fix your PC remotely.

PHISHING FACT #1

Google, PayPal, Yahoo and Apple were the most impersonated companies in 2016.
Of all phishing sites detected between January and October 2016, Google was the most-impersonated brand (21%), followed by Yahoo (19%), Apple (15%), PayPal and Wells Fargo (both 13%) *(Samarati, 2016).*

For further details please contact: Jackie McLinden – ICT Training and Support Officer on E: jackie.mclinden@bhs.org.au P: 5320 8987



SEE SOMETHING - SAY SOMETHING

There is no tech defense against phishing attacks that guarantees security because a staff member decides to click the malicious link. The more that staff are aware of phishing and its risks, the less likely they are to swallow the bait – and avoid putting BHS at risk.

Do **no**t click on any links or open attachments from an email claiming to be from your bank or another trusted organisation and asking you to update or verify your details – just press delete and contact the IT helpdesk on ext. 94786 OR helpdesk@bhs.org.au

PHISHING FACT #2

Phishing is the fastest growing social media threat due to the ease of account creation of known brands. 40% of accounts on Facebook and 20% on Twitter that are representing the top 100 world companies are unauthorised

(Schneier, 2016).

PC TRAINING

Do you need assistance accessing a computer? Would you like support accessing / managing your emails?

Would you like to view your 'Leave' or 'Training' status regularly?

For department or small group support please contact the Jackie McLinden - ICT Training and Support Officer on ext. 98987

OUTLOOK TRAINING

Tues June 6th
Wed June 14th
Thurs June 22nd
Wed June 28th
All Sessions commence at 2pm in the Library IT Training Room- Bookings are essential.

For department or small group support please contact: Jackie McLinden - ICT Training and Support Officer on ext. 98987

NEED HELP?

Staff can contact the I.T Helpdesk Mon – Fri 0800 – 1630:
P: 5320 4786 ext. 94875 OR
E: helpdesk@bhs.org.au