Emerald ICT
Complete Computer Solutions

October 2016

NEWSLETTER

From October 2013 through February 2016, US law enforcement received reports from 17,642 victims of phishing attacks. This amounted to more than $2.3 billion in losses.

Source: FBI.gov

5 Red Flags of Phishing Emails: Think Before You Click

A single click can be the difference between maintaining data security and suffering massive financial losses. From the moment just one employee takes the bait in a phishing email, your business is vulnerable to data breaches and extensive downtime.

Quickly spot the red flags and put phishing emails where they belong:

1. Poor spelling and grammar

While occasional typos happen to even the best of us, an email filled with errors is a clear warning sign. Most companies push their campaigns through multiple review stages where errors are blitzed and language is refined. Unlikely errors throughout the entire message indicate that the same level of care was not taken, and therefore the message is likely fraudulent.

2. An offer too good to be true

Free items or a lottery win sure sound great, but when the offer comes out of nowhere and with no catch? There's definitely cause for concern. Take care not to get carried away and click without investigating deeper.

3. Random sender who knows too much

Phishing has advanced in recent years to include 'spear phishing', which is an email or offer designed especially for your business. Culprits take details from your public channels, such as a recent function or award, and then use it against you. The only clues? The sender is unknown – they weren't at the event or involved in any way. Take a moment to see if their story checks out.

4. The URL or email address is not quite right

One of the most effective techniques used in phishing emails is to use domains which sound almost right. For example, [microsoft.info.com] or [pay-pal.com]

Hover over the link with your mouse and review where it will take you. If it doesn't look right, or is completely different from the link text, send that email to the bin.

5. It asks for personal, financial or business details

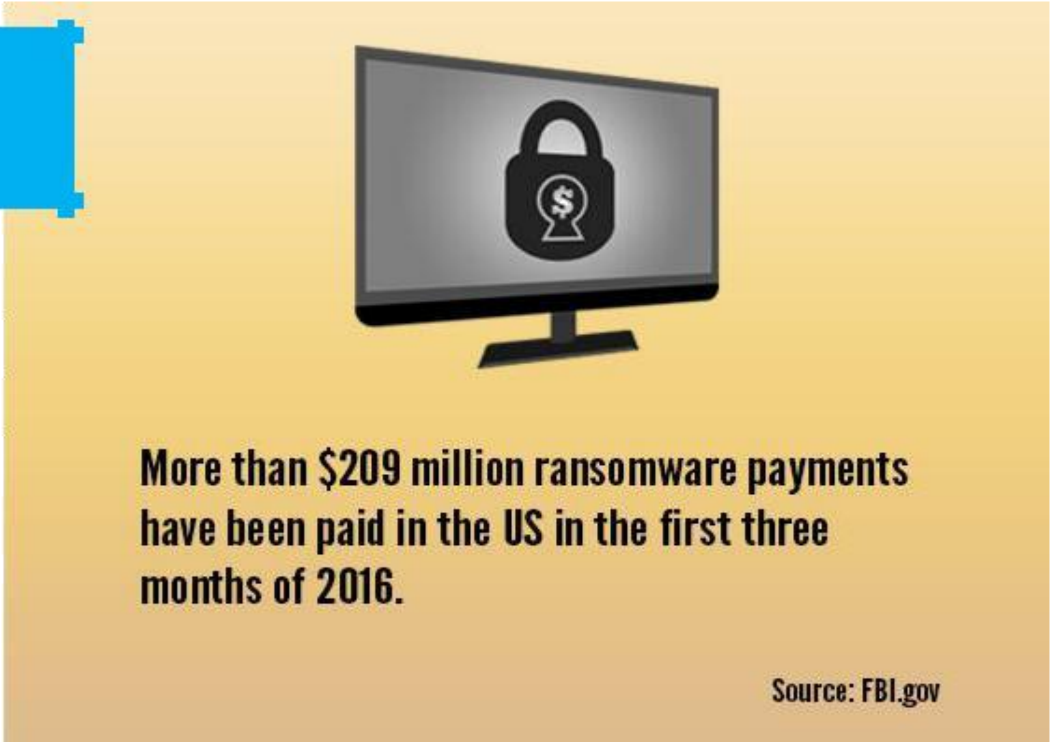
Alarm bells should ring when a message contains a request for personal, business or financial information. If you believe there may be a genuine issue, you can initiate a check using established, trusted channels.

While education is the best way to ensure phishing emails are unsuccessful, a robust spam filter and solid anti-virus system provide peace of mind that your business has the best protection available.

Give us a call to discuss how we can secure your system against costly phishing attacks. 0113 2579992

Welcome to our first feature of our Tech Newsletter! As our valued customer, you'll be getting tips and tricks on how to stay safe online and become a master of your computer.

No Payment = No Password = No Data.



More than $209 million ransomware payments have been paid in the US in the first three months of 2016.

Source: FBI.gov

Could Your Backups Survive A Ransomware Attack?

More and more businesses and organizations are getting stung by ransomware demands. Hospitals, schools, social networks…some days it seems like an epidemic that leaps around arbitrarily, and hackers are raking in millions.

Tallied across the word…billions.

Ransomware attacks are devious in their simplicity. A user in the target business is tricked into opening a file, usually through a phishing email or download. The file contains malware which instantly encrypts your data and demands money in exchange for the password.

No payment = no password = no data.

All of the target businesses should have backups, which they could simply revert to without paying any money, but the FBI reports more than $209 million was sent to hackers in the first quarter of this year alone. Keep in mind, this was just payments within the US, and only counts those who came forward.

Last year it was only $25million.

Aren't backups helping?

Sometimes the backup solution fails and the data can't be retrieved. This is Particularly true in cases where the solution has been in use for years and something failed along the way.

In other instances, the target business has a backup that can be restored, but it doesn't include everything they need for full recovery.

Finally, and the most common reason so many businesses are forced to pay the ransom: the ransomware attack affects the entire system – including attached and synchronized backups. If the backup is also caught in the ransomware encryption, it becomes useless as a recovery method and the only options are to pay or lose the data forever.

Each day spent trying to recover the data is a drain on valuable business resources and in many cases, results in massive revenue loss.

The only defense is to block the malware before it can infect the first workstation, and then continue the protection with a comprehensive backup strategy for all workstations and servers.

Give us a call to discuss how we can help secure your business against ransomware today 0113 2579992