KNOWLEDGE BRIEF

GDPR: EMAIL SECURITY

GO PHISHING!

Despite being one of the oldest internet scams, phishing continues to unleash mayhem in businesses.

The dreaded bogus links in incoming emails can trigger everything from banking fraud, to ransomware, to theft of your dteails (e.g.Office 365 login

SPAMALOT

Ordinary spam is a nuisance, but the real danger lies in the malware that can be delivered by spam: Last year over 70% of ransomware was via spam.

COSTALOT

Compromised business email scams, will exceed $9 billion In global losses this year, according to security vendor Trend Micro.

T'INTERNET

Also remember to protect your network from Web-based malware and viruses, and shield your employees from offensive content.

TRUSTWORTHY

Look after your customers data in emails and they'll trust you to do business with.

SPRING CLEAN YOUR MAIL BOX

Over 120 billion business emails will be sent this year - Spam, phishing, malware and ransomware are just some of the hazards these emails could carry.

As long as businesses keep sending and receiving emails, the bad guys will keep using them to try and attack the communication line of businesses.

Worst case scenario?
Your email is hacked; sensitive data stolen, your reputation is damaged - you go out of business.

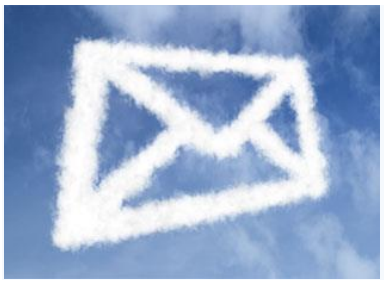
Best case scenario?
Less spam, phishing and data theft … showing you look after personal data – an important step towards GDPR!

CLUTTER FREE

It is imperative to have a multi-layered email security policy in place – whether you use on-premise or cloud-based email solutions, the same security precautions apply:

- ✓ Anti-virus and spam protection is a must – up to 90% of emails sent are spam
- ✓ Also look for solutions that defend against malware, ransomware and targeted email attacks such as spear phishing and spoofing attacks
- ✓ Consider greylisting (prevents unknown apps launching) as well as white and blacklisting
- ✓ Use email encryption when sending confidential emails to protect data and automatically enforce GDPR compliance requirements.
- ✓ Educate employees on tactics attackers use to help them identify threats - do not open email from unfamiliar senders. When in doubt, delete without opening it. Verify first before opening any attachments.

CLOUD DREAMING



Consider cloud-delivered, as-a-service email solutions that major on ease of use: no-maintenance deployment, 24 x 7 updates, patches and hot-fixes delivered automatically by the vendor.

Emails are filtered and scanned prior to it reaching the recipient, so threats are intercepted before they touch your business's network. There's nothing to remediate, no spam to archive, nothing to clean up.

BUT remember to Secure IT & Back IT up!

DO NOT COMPROMISE

We're not GDPR experts but we DO know about the best email-security solutions!

- ✓ We provide solutions with technology based on artificial intelligence that stops email scammers impersonating executives protecting you from business email compromise attacks.
- ✓ Solutions use Time-of-click URL blocking: malicious links are analysed and blocked before threats, like ransomware, can execute or reach the user.
- ✓ Our email solutions are part of a wider layered security approach that shares security intelligence with other layer and application security products. (We only provide solutions that work together across all layers).

CONTACT US TO LEARN MORE ABOUT HOW WE CAN HELP YOU WITH CYBER-SECURITY & GDPR

0207 118 0900 | sales@ngexperts.net | www.ngexperts.net

ngexperts UNIFIED COMMUNICATIONS