DRAGON

10 SIMPLE STEPS TO CYBER SECURITY

In a recent survey of our clients, we found that IT security was growing area for concern for many small and medium sized businesses. If you feel you are not doing enough to protect your business from a cyber attack and you don’t have the in-house resources or skills to manage your cybersecurity, Dragon IS can help you with cost-effective path to a secure network. To get started, here are the 10 simple steps we can help you take towards reducing the risk...

Dragon IS, 6 Bassett Court, Newport
Pagnell, Milton Keynes, MK16 0JN
T · +44 (0)330 363 0055
W · www.dragon-is.com

UNDERSTAND YOUR DIGITAL FOOTPRINT

Before implementing a new Cybersecurity solution we carry out a full IT audit to fully understand your business's digital footprint. With this information we can recommend a Cybersecurity policy to compliment and support your working processes.

PROTECT INFORMATION & NETWORK SECURITY

Protect your network from attacks by installing end point protection such as a Unified Threat Management (UTM) Gateway and firewall with content filtering at the perimeter of your network.

TRAIN YOUR EMPLOYEES

Establish basic cyber security principles and train and educate your employees on security best practice, alongside appropriate internet behaviour and acceptable use of company equipment.

DATA BACK-UPS

Implement regular back-ups of important business data and information. Store back-up off site in the cloud and regularly test your data back-ups and cloud applications back-up.

UPDATE & MAINTAIN NETWORKS

Download and install software updates and patches for your operating systems and applications to ensure the secure configuration of all of your systems.

SECURE YOUR NETWORKS

Secure your Wi-Fi network and make sure it is secure and hidden. Use and regularly update antivirus and antispyware software on every computer used in your business.

USER MANAGEMENT

Protect your networks from internal threats by setting up password-protected individual user accounts for each employee, including limits for the use of portable storage devices, employee access to data and information, and authority to install software.

RISK & DISASTER MANAGEMENT

Assist with establishing a robust incident response and disaster recovery plan should the worst should happen. Test and review your disaster plans on a regular basis.

PROACTIVE MONITORING

Constant monitoring of your networks allow us to spot unusual activity and apply the necessary protections to stop any data breaches or disruption to your business.

SECURE MOBILE WORKING

Develop a mobile device action plan and install encryption and mobile device management software in all mobile devices to protect data in transit and from theft or external breaches.

10 SIMPLE STEPS TO CYBER SECURITY

www.dragon-is.com

DRAGON