Safe Remote Working – Cyber Security Advice to help protect your Organisation.

Joe McGivern, CEO, supportIT

supportIT

10 Manor Street Business Park, Manor Street Dublin 7
T: +353 (0) 1 902 2112 E: enquire@supportIT.ie W. www.supportIT.ie

ISO 9001 CERTIFICATION EUROPE™

supportIT

1. about me

- Security Consultancy/Audits/Compliance
- Managed Support Services Have Changed
- Helping Clients Manage the Evolving Threat Landscape
- Disparate Workforce (NFP's)/Remote Locations & Users
- Reliance on different types of Devices
- Software as a Service allows for a end-point support and mgmt
- Microsoft Silver Partner/Grants & Donation Programs

supportIT

2. types of attacks?

- **Malware Phishing** – Tricking a user into downloading a malware attachment.
- **Ransomware** – Links into Phishing, Criminals Encrypt data then ask for money to decrypt
- **Vishing** – Trying to extract valuable information/bank details by pretending to be someone else over the phone.
- **Spear Phishing** – Researching a high value target(in Finance etc), developing a convincing backstory with personal information and intercepting an email conversation.
- **Business Email Compromise** - Using a phony email with a contrived pretext to request payment
- **Clone Phishing** – Replacing a single element of a legitimate email with malicious one to create a nearly identical email.
- **Smishing (SMS + Phishing)-** Delivering a malicious link via a short code to a Smartphone
- **Pharming** – Rerouting a legitimate traffic to an attackers page.

*Source Webroot

3. why the increase in Cyber Attacks?

- Attacks have tripled since this time last year.*
- End Users are being attacked because they are more vulnerable/People are working disparately/separated from their processes & colleagues
- Reliance on Technology During the Pandemic/Technology can be easily used to impersonate
- Home machines are more vulnerable/Used by more than one person/Not Patched or Updated

*Source Webroot

4. how to protect your org: **awareness**

- People are the weakest link /Bank Account details
- Clear Policy and procedures
- Staff Training to ensure staff are aware of the latest threats
- Highlight attempted email scams so staff can know what to look out for
- Alerts work well for creating awareness

5. how to protect your org: cont'd

- Agree policies that relate to all devices/BOYD policy/Protection
- Strong security policy to enforce user and device rules
- Strong password policies should also apply to 3rd party applications being used in the business, like CRM applications and Finance applications.
- Conditional Access

6. threat protection solutions

Anti-Virus

The best products are paid solutions with proven detection rates/Make sure that you include phones, tablets, laptops/Our recommendation is Webroot.

Multi-Factor Enablement

This is activated within the application itself/best practice to ensure your application is secure, particularly if you store personal identifiable or finance data.

Data Loss Protection

For those organisations that have more stringent compliance /DLP is a built-in feature of Office365/activated through the management console.

7. questions

contact: www.supportIT.ie

contact:
jmcgivern@supportIT.ie

10 Manor Street Business Park, Manor Street Dublin 7
T: +353 (0) 1 902 2112 E: enquire@supportIT.ie W. www.supportIT.ie