

Cyber Security For Small & Medium Business



Cybersecurity is a growing concern for SMBs in 2017

A Question of Identity...



Physical Me



The Digital Me

Digital Footprint

- Websites
- Online Shopping
- Banking
- Social Media
- Public Directory Listings
- Instant Messaging



*We trade Convenience for Loss of Privacy
which has Commercial Value*

Why Care? - I have nothing to hide!

Protect your Reputation
and that of your business.
Not everything you put
online is for every audience.

Decide how you want your
information shared - Medical
information, Religious Beliefs, etc.

Corporates now commonly share
your data for marketing purposes
and with Governments!

Identify
Protection

Does that expose you to potential harm?...

Your Footprint can be Abused

- Credit Vetting based on spending habits
- Identity Theft - Websites being Hacked
- Insurance Profiling
- Intelligence Organizations
- Super-Surveillance - Mobile tracking at a Riot in Kiev



Time To
Take Action

Train your Employees

- Establish basic security practices.
- Appropriate Use of Equipment
- Implement Rules of Behaviour



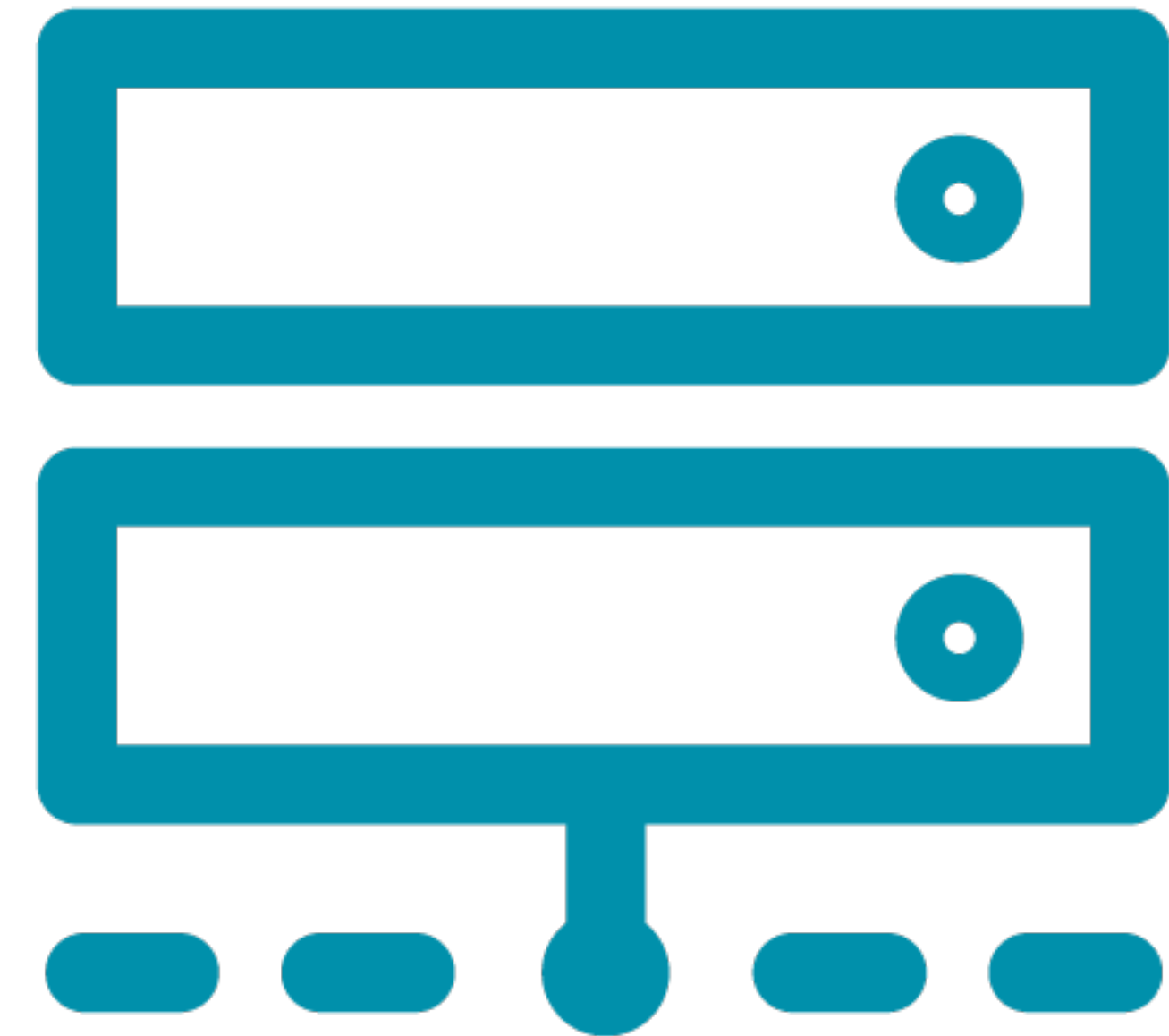
Security Best Practices

- Strong Passwords
- Internet Use Guidelines
- Security Policy for Handling Customer Data



Appropriate use of Equipment

- Safeguarding Devices
- Secure Destruction of Media
- Being mindful of how and where data is stored.



Establish Rules for Data that is Relevant to your Industry

- Speak to Industry Representatives
- Risk Analysis - Understand the where the risks are.
- Implement and Monitor Rules to Comply



A person's hands are shown holding a smartphone and a pen over a notebook. A teal circle is overlaid on the image, containing the text "Going Forward". The background is dark with colorful bokeh lights in shades of green, yellow, and red.

Going
Forward

DRAGON 

Protect Information, Computers & Networks

- Keep devices up to date
- Install Endpoint Protection
- Network - Firewalls with Content Filtering and AV
- Install Software Updates when they become available
- Mobile Device Action Plan
- Server/Cloud Level SPAM Filtering and Virus Checking



Data Backups

- Implement a Regular Data Backup
- Not just Critical Data
- Store the backups offsite
- Regularly Test your Backups
- Protect Cloud Applications with Backup



Control Access

- Control Physical Access to premises, laptops, servers etc.
- Each employee needs their own account. Restrict the account to the job role.
- Remove Admin Privileges



Limit Access

- Do not provide any one employee access to all data systems
- Limit authority to install software
- Limit use of portable storage devices on computers - data theft
- Control or Monitor employee use of personal accounts when on a work computer



Passwords & Authentication

- Use different passwords for different sites
 - Password Manager
- Change Network passwords every three months
- Secure your Wi-Fi
- Use Two Factor authentication if available



Passwords & Authentication

“Passwords are like underwear: you don’t let people see it, you should change it very often, and you shouldn’t share it with strangers.”







Check out our 10 Step Cyber Security PDF today