Keys to Safe and Secure Remote Work

1.  Secure remote connection
2.  Dual/Multi Factor Authentication (2FA)
3.  Is your email safe and secure?
4.  Backup, Backup, Backup

1. Secure remote connection

Objective: create a secure connection to your office computers without compromising productivity

- RDP - Remote Desktop Connection - allows you to 'take over' another computer – there are several ways to create an RDP connection: RDP Software, Logmein, Gotomypc, Splashtop, Teamviewer
- VPN - Virtual Private Network – creates a protected connection – this is the recommended way to establish an RDP

2. Dual/Multi Factor Authentication (2FA)

Objective: minimize your risk of compromise when accessing programs and information

Dual/Multi factor authentication is a security method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism. Dual/Multi factor is recommended when accessing:

- Remote Desktop Connection
- Email
- Applications
- Websites

3. Is your email system safe and secure?

Objective: enhance the security of your email system by flagging and prohibiting suspect communication

- Does your email system prevent spam, phishing, spoofing?
- Do you have the ability to send & receive secure & encrypted emails? Sending secure email protects you and your client's or recipient's information.
- Common email mistakes:
  - Sending passwords through email
  - Sending credit card information through email
  - Sending confidential information and attachments
  - The average small business thinks they are not a target

What can you do as a small business to minimize your risk?

Be educated on cyber threats!

Spam/Junk Email

Spam is **45%** of all emails sent

Spam costs businesses a mind-blowing **$20.5** billion every year

Spam leads to:

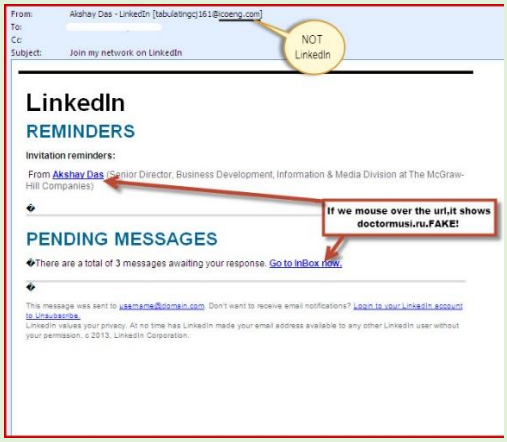
- Revenue loss
- Decreased productivity
- Lost emails/Hacking

What is Phishing?

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Spoofing

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source.



4. Backup, Backup, Backup

Objective: have a plan in place to ensure your business can survive a hardware & software failure or ransomware attack

- Where is all of your data being stored?
- Is your email getting backed up?
- Is your cloud data getting backed up?
- What happens if your server crashes?
- Do you have a disaster recovery plan?

For more information and recommended solutions, call Right Click Solutions.

Right Click Solutions LLC
small business computer consulting

27 Radio Circle Drive, Suite 104 Mount Kisco, NY 10549 (914)242-3212 www.RCSLLC.net