9 DIGITAL SECURITY ESSENTIALS

FOR SOLOPRENEURS, MICRO-BUSINESSES, AND...WELL, EVERYONE!

1 Take Ownership

Take responsibility for what is going on in your business. Step up and oversee everything, making sure you're protected.

Know Who Has Access & What They Have Access To

If you give someone access to your account, make sure you revoke their access/change your password when they don't need access anymore.

Know What Accounts You Have Out There, Your Software, Etc.

Make a spreadsheet or document to keep track of everything you need to make your business's online presence work.

2 Keep Software Up To Date

Updates usually contain security patches that fix vulnerabilities. Hackers love taking advantage of vulnerabilities, so don't run outdated versions!

Update Your Internet Browser, Your Apps + Your Operating System

Updates come out regularly, so stay on top of it!

Update Your Website

If you use a closed-source platform, like Squarespace or Shopify, updates are generally taken care of for you. If you use a self-hosted Wordpress site, you are responsible for updates.

3 Back Up Everything

Phones. Laptops. Your website. Important emails. Tax documents. Everything.

Data Loss Happens.

Sometimes it's on accident, like your computer's hard drive wears out. Having everything backed up makes this easier to deal with.

Back-Up Options:

Use external hard drives, USB flash drives, the cloud, physical copies, and back-up services.

4 Use Safe Passwords

Don't underestimate this!

Don't Use These Unsafe Components:

- The word "password"
- Your name
- Your brand's name
- Names of family members
- Your birth date
- "123" or other consecutive letters/numbers

The Best Passwords Are:

- A combo of words, numbers, symbols, and uppercase/lowercase letters
- Long! 16+ characters
- Unique: don't use the same password for every account you have

5 Set Up 2 Factor Authentica-

This adds an extra step and layer of protection to the login process.

2FA May Already Be Set Up On Some Accounts

It seems to be automatically enabled on Google accounts, for example.

Add 2FA To Your Website, Social Media, Etc.

Google *"2 factor authentication + [the platform in question]"* for instructions.

6 Be Alert For Suspicious

Remember the Nigerian Prince email scam? It's still around, along with a whole host of other, increasingly believeable scams.

Keep Your Cool

Email scammers rely on us not being savvy to their ways. Don't react emotionally - if you get an email that seems a bit "off," stay calm and hit Google to see if it's a well-known scam.

Be Cautious Of The Weird/Unexpected

Use caution even if the email looks like it's coming from a sender you recognize.

7 Prevent Email Spoofing

Email spoofing involves the creation of messages with a forged sender address. Emails could look like they are coming from you@yourdomain.com, but they actually aren't.

Set Up The Right Records

• SPF • DKIM • DMARC

Use A Throwaway Email For Registrations

Supposedly, this can help prevent your regular email address from getting on lists that are used for sending spoofed emails out in bulk.

8 Be Mindful Of Your Data Storage

If you're doing business online, you're likely collecting sensitive data like email addresses, physical addresses, full names, and so on.

The rest of these digital security tips will help you safeguard this info; in addition, be careful that you aren't storing any sensitive data in places where it is public, like where it can be picked up by search engines.

9 Audit Often & Stay On Top Of It!

Don't wait until your website gets hacked or your email gets compromised to deal with digital security.