Top 7 Email Safety Tips For SMBs

CORPORATE TECHNOLOGIES GROUP

1 Pause before you act.

If a message tries to rush you or make something feel “urgent,” slow down. That pressure is one of the attacker’s favorite tools.

2 Check the sender carefully.

Look for tiny misspellings, extra letters, or domains that are just a little “off.” Those little details matter.

3 Don’t trust links just because they look “right.”

Hover over them to see where they really go, and if it feels even slightly weird, don’t click.

4 Verify payments and account changes through another channel.

Unexpected invoices, new bank details, or “please pay today” emails should always get a quick phone call before money moves.

At Corporate Technologies Group, caring about security is not a separate add-on. It is part of how we help you run a better, safer, more connected business. Our goal has always been to help clients work toward solutions that integrate and connect mobile devices, computers, and their full staff so everything works together cleanly and reliably under one umbrella.

5 Use long, unique passwords.

Reuse turns one compromised account into a chain reaction. A password manager makes this easy.

6 Be cautious with attachments and even internal emails.

If it wasn’t expected, or it doesn’t make sense in context, treat it carefully — spoofing can make a message look like it came from someone you know.

7 Turn on multi-factor authentication whenever it’s available.

It stops most account takeovers cold, even when a password leaks.

Want to make sure your email can’t be faked? Call us at **330-655-8144** or email **info@ctgusa.net**, and we’ll walk through what you have in place and what comes next.

5344 Darrow Road Hudson, Ohio 44236 | info@ctgusa.net | 330-655-8144 | https://ctgusa.net