SECURITY

INTRODUCTION

Security plays a large part in our daily lives, from national headlines of data breaches down to your own email. Using easy to follow best practices, small business owners can avoid many of the vulnerabilities hackers use to infiltrate your networks, bank accounts and devices.

OPSEC CHECKLIST

- Use unique password for each online service. Do not re-use passwords, not even **once**!
- The passwords you do use **need to be long**. They don't need to look like gobbledygook, ex: FKSNHOSAy09wh - you can use readable sentences like BatteryHorseStaple10 - which is easier to remember but more complex.
- Use **two factor authentication** (2FA) where available. For your most critical services (banks, email) enable 2FA. This requires not only your password, but an additional code (from your phone) to login.
- Do not click links within emails! **Don't trust emails** asking you to login to confirm even a legitimate sounding action. Open your browser, navigate to the official website, and then login from there.
- Scan and update your devices, especially your **Windows PC, and Apple Mac**.
- **Change your important passwords**. The first tactic for hackers is to try a leaked password with your email everywhere they can!

HAVE YOU BEEN PWNED?

A free and very useful tool has emerged to track the recent huge personal information data breaches. It's called **Have I been Pwned** and all you need is your email and ... **yes, you've been pwned.** Don't freak! Just make sure to change your passwords.

COLEWEBDEV WHITE PAPER

OPERATIONAL SECURITY
BEST PRACTICES FOR SMALL BUSINESS