Your Password Safety Checklist

We've covered a lot of ground! To make it easier, here's a simple checklist of key steps to keep your passwords (and accounts) secure. You can even print this out or download it for reference:

- [ ] Use a unique, strong password for each account. (No repeats! Length 12+; mix of words, letters, symbols.)
- [ ] Enable two-factor authentication (2FA) on all accounts that offer it (especially email, banking, social media).
- [ ] Store passwords in a reputable password manager. (Stop writing them on sticky notes or saving in plain files.)
- [ ] Never click suspicious links or give out passwords/codes to anyone who contacts you unsolicited.
- [ ] Avoid using personal info in passwords (no names, birthdates, etc. – too easy to guess).

- [ ] Regularly update important passwords, especially if you hear about a breach. Don't recycle old passwords either.
- [ ] Don't share passwords via email or text. If you must share with a family member, do it securely (in person or via a shared manager vault).
- [ ] Educate yourself and your family/team about phishing scams and safe browsing habits.
- [ ] Keep your devices secure, since saved logins reside there: use device PINs/passwords, update software, run antivirus if applicable.

(Feel free to download the full checklist here for a handy one-pager to follow. And check out our Password Safety Infographic for a visual summary of these tips in a fun format!)