A few useful tips for getting people onboarded to RC 2FA workflows:

1. Many people won't have a 2FA app installed on their phone or machine
2. Some people who *do* have one installed may have work-associated restrictions

2FA Apps

	Android	iOS	MacOS	Windows	Linux
Aegis	Y				
KeePassDX	Y				
Google Authenticator	Y	Y			
KeePassXC			Y	Y	Y

1. Google Authenticator is easy, and allows for using without attaching to google email
2. Aegis is also quite easy, play store or F-droid
3. All varieties of KeePass will be more confusing, as it's both a password vault and 2FA mechanism.

Sharing Seed

If you're helping someone get 2FA set up, at some point you'll need to convey the seed. If you have a signal connection with the person: easy. If you don't, it's more difficult.

One way to easily share it from your machine to a mobile device is to generate a QR code using the otpauth: URI scheme

This script will take standard input so as to not leave information in your terminal history, should work in bash and zsh

```
printf '2FA App Entry Name: '; read -r A
printf 'Issuer: '; read -r I
printf 'Secret: '; read -rs S; echo
A=${A// /%20}; I=${I// /%20}; S=${S// /}
printf 'otpauth://totp/%s:%s?secret=%s&issuer=%s' "$I" "$A" "$S" "$I" | qrencode -t ansiutf8
unset A I S
```