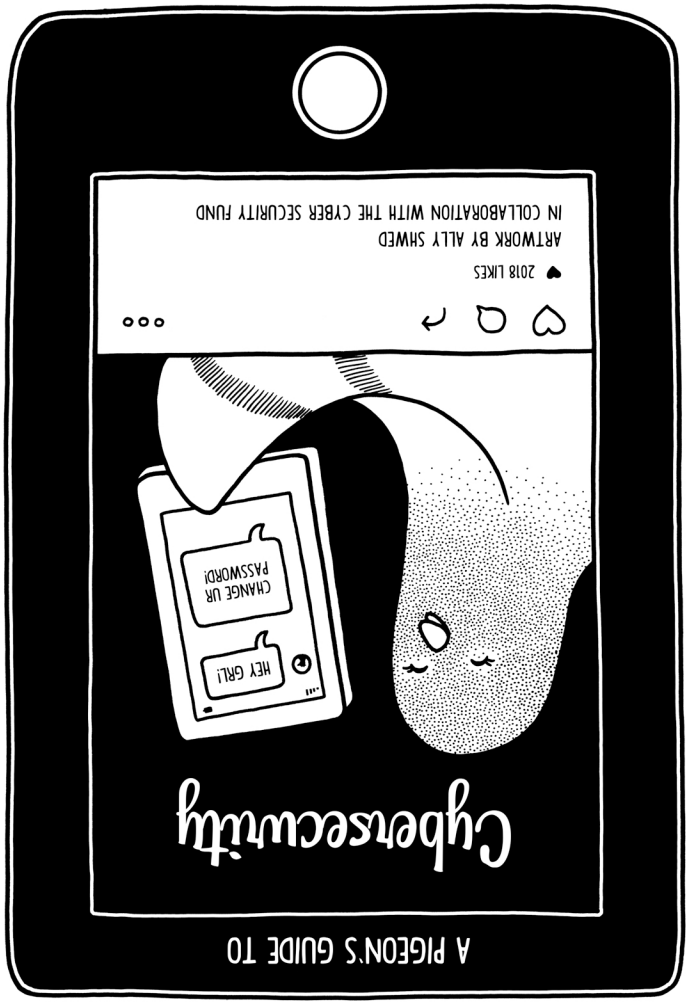
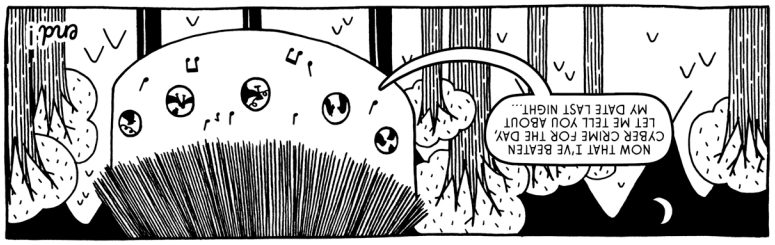
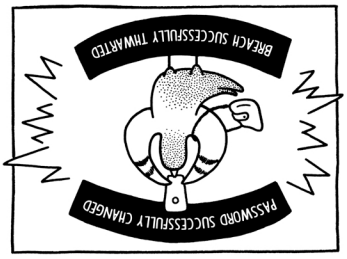
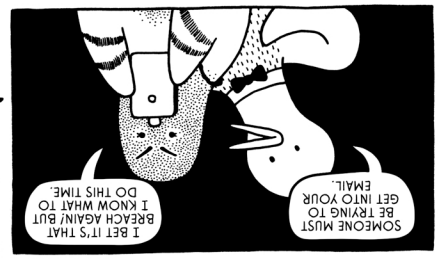
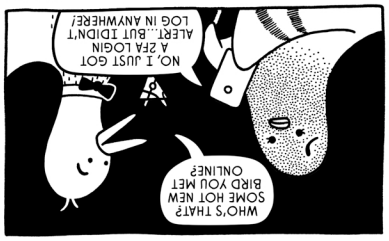


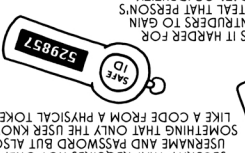




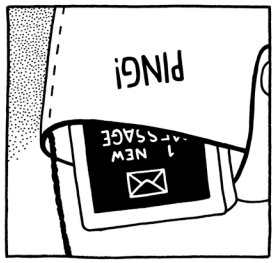


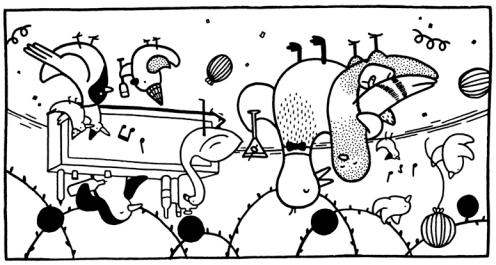


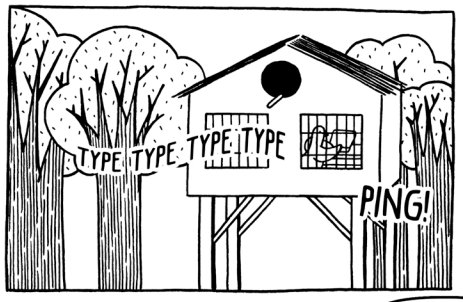
TWO-FACTOR AUTHENTICATION, ALSO KNOWN AS 2FA OR MULTI-FACTOR AUTHENTICATION, IS AN EXTRA LAYER OF SECURITY THAT REQUIRES NOT ONLY A USERNAME AND PASSWORD BUT ALSO SOMETHING THAT ONLY THE USER KNOWS, LIKE A CODE FROM A PHYSICAL TOKEN.

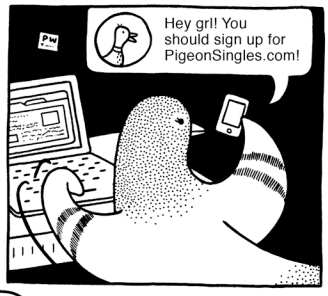


THIS MAKES IT HARDER FOR POTENTIAL INTRUDERS TO GAIN ACCESS AND STEAL THAT PERSON'S PERSONAL DATA OR IDENTITY.









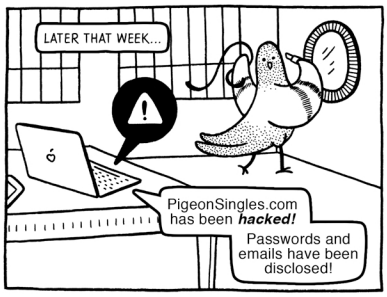
"PASSWORD"?
EASY TO REMEMBER, BUT TOO EASILY GUESSED!

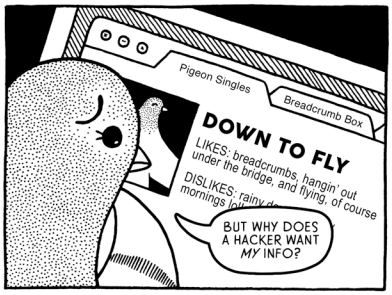
"PASSWORD123"?
NOT *THAT* MUCH BETTER. I CAN GET MORE CREATIVE THAN THIS!

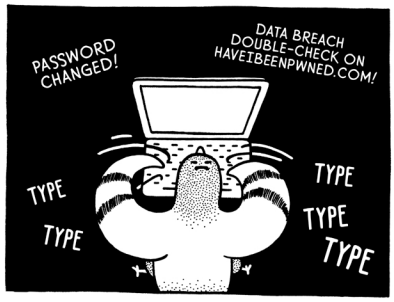
"BREADCRUMBS12"?
A LITTLE BETTER, BUT A COMPUTER CAN QUICKLY MAKE A FEW MILLION GUESSES TO FIGURE THIS ONE OUT.

"GFW#3EEKOWJ"?
NO ONE WOULD GUESS THIS ONE!

"LIBERTYBELLCATNIP POTATOBREAD"?
A REALLY LONG PASSWORD COMPOSED OF WORDS IS OFTEN AS SECURE AS A SHORTER ONE WITH NUMBERS, SPECIAL CHARACTERS, AND MIXED-CASE LETTERS! OF COURSE, THE WORDS NEED TO BE RANDOM AND HARD TO GUESS.



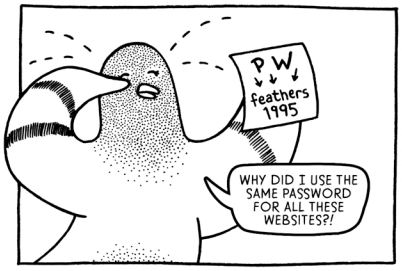


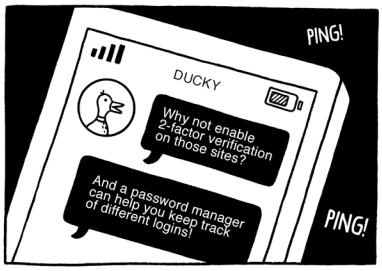


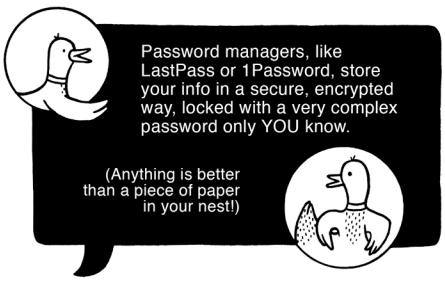
';--have i been pwned?

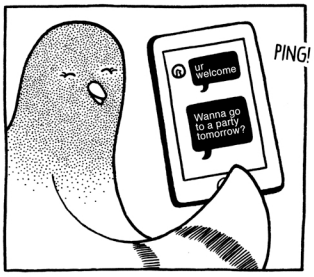
Check if you have an account that has been compromised in a data breach

You've been compromised on CarrierPigeon.com, crumbdelivery.com, GuttersForRent.com, and HatchlingCare.org!









QUESTIONS? HELP@CYBERSECURITYFUND.IO