Portfolio Note: This article was written for a major password and security company as they reconsidered the nature of their blogging and outreach program.

The idea was to demonstrate the ability to take complex topics, like password security, and create something simple to follow and understand for nontechnical users using plain language and helpful resource links.

The original article included a call to action, which I've removed, but linked back to the company website as part of a conversion initiative.

Better Online Security in 3 Easy Steps

Even if you're a power-user, securing your online footprint can feel like a chore. That's not your fault.

Technology moves quickly, and keeping up with the tricks and schemes that hackers use to steal your digital identity might feel like more than you bargained for when you first logged into Facebook. (And, speaking of Facebook, you should really change your password.)

Let's talk about three quick and easy steps you can take for better online security in 2019.

1. Create Easy-to-Remember Passwords

There's a reason we use the same passwords over and over again: Coming up with a new, memorable password is hard!

Unfortunately, it's also necessary. When you're creating a password, it's important that you don't just use whatever pops into your head. It's too easy for automated password crackers to solve. Use something random but memorable for your most important passwords.

One method I often recommend is finding a memorable sentence or song lyric, then changing letters to numbers and specialized characters. So if my password is [allyouneedislove] from the classic Beatles hit, it becomes [@llY0uN33di$L0v3].

It's the same phrase, but I've changed some letters to special characters (a to @, s to $) and added capitalization to the first letter of every word. A password like this is easy to remember, but deceptively hard to follow if you don't know how to make it — and even harder for automated password crackers just plugging in random numbers.

You can also use Diceware, a system which allows you to create a randomly-generated password by rolling dice and comparing your rolls to a list of words. It's simple, easy to use, and great if you love board games!

2. Occasionally Change Your Password

If you're like most people, you only change your password when a website forces you to do so either because of a data breach or because you forgot your current password. (Guilty!)

But really, we should all be more frequent about occasionally updating our passwords.

And don't get us wrong, we're not saying that you should make it a once-a-week, Friday-date-night sort of thing. Even the

National Institute of Standards and Technology only recommends changing passwords once every 90 days.

Keeping password changes infrequent avoids security fatigue and stops you from forgetting all the passwords you've created. But remember: when you change your password, you shouldn't reuse older passwords. Create a new one, make it easy to remember, and don't use it anywhere else.

Sounds exhausting, right? Our team is dedicated to security, and even we know how tedious that sounds. Plus, if you've been online for even a small amount of time you've probably created more passwords than you want to keep track of.

That's why we recommend:

3. Use a Password Manager

You might've heard about password managers like 1Password by now. Password managers are designed to help you secure your online identity by creating strong, randomized passwords like this one from the 1Password password generator: [pTk)VaD9@YWh*t:~Ts~k].

Can't remember that? No problem. That might actually be a benefit, according to some security experts.

Password managers remember complex passwords along with the rest of your login information for any website you visit (with permission). When you return to the website and need to log in again, the password manager fills in your information so you don't have to.

Typically, password managers are also more secure than your browser's password autofill — which is a security risk — because they still require you to do something before filling in forms on your behalf.

Using tools can help you secure and protect your digital footprint more easily. You should still follow best practices, but using password managers and alert tools like Watchtower to find passwords in need of maintenance make online security far less tedious.

Bonus: Don't click links delivered via email or text.

While everything we've mentioned so far can help you be more secure online, we wanted to add a quick bonus step that's less about password creation and more about password protection.

Scammers and hackers are always looking for ways to trick an unassuming user into willingly providing their login information. Why go through all the trouble of cracking a password when you can just trick someone into handing it over?

A tried and true method is "phishing". To do this, scammers send a fake email or text message while posing as a service provider you're likely to use — for example: Facebook.

They're hoping that you'll click on the link they give you and enter your information into a fake version of a website. When you do that, you've just given the bad guys everything they need to steal your online identity!

Phishing is a deceptively clever trap to fall into, even if you're familiar with modern security procedures. You can see this technique in action right here.

In short: Don't click on links delivered via text message or email unless you're expecting them!

If you get an email from Facebook telling you that your password has been compromised, don't click the link in the email to reset your password! Open your web browser, and go to Facebook directly. See if you can log in using your existing credentials or if Facebook forces you to reset your password.

Verify the need to take action independently if you're having trouble determining whether or not an email is real or fake.