**Tips and tricks to secure your clicks**

**Image:** Included in toolkit.

**Alt Text:** Two figures putting together a puzzle of a padlock.

Bad actors are always finding new and sophisticated ways to steal information. Now more than ever, it’s important to augment your thinking and creativity regarding password protection.

Passwords are often the only locks on your account door, and with such a vast security threat landscape, you need more than just a lock to minimize cyber risks. Adding an extra layer of protection with [multi-factor authentication](https://news.va.gov/110281/online-scammers-steal-information/) (MFA) can block over 99.9 percent of cyber-attacks[.](http://./)

What is multi-factor authentication?

Multi-factor authentication, sometimes known as two-factor authentication, is an extra layer of protection on your account. Each time you sign into a VA website or app, you’ll use multi-factor authentication to verify you’re you. You’ll do this using a device to which only you have access, such as your mobile phone.

Prevent identity theft and fraud when you enable MFA. A bad actor may guess or steal your username and password, but multi-factor authentication will stop them.

For a guide to implementing MFA, [play our video on multi-factor authentication (YouTube)](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3Dt85bt7Pmlvg&data=05%7C01%7C%7Cb006c09af1f84b9a54f008db7e659cea%7Ce95f1b23abaf45ee821db7ab251ab3bf%7C0%7C0%7C638242747102960692%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=%2BjAbb06mjL3oVDm51ACjiAWvG7hVH4wzGLLKMjs8g2k%3D&reserved=0).

Are your accounts at risk?

Most likely because password reuse can present security issues like phishing and breaches. Chances are you’re reusing the same credentials across multiple sites, which is one of the leading security problems with passwords. The U.S. Department of Interior found that [watchdog staff members decrypted the passwords](https://fedscoop.com/interior-password-management-failings/) for 16 percent of the agency’s user accounts in 90 minutes, while 5 percent of active credentials at the agency used a variation of the word “password” in their password.

A double step to double check

Enabling MFA on your accounts is a significant line of defense that can lessen your chances of getting hacked. This is because even if a malicious cyber actor cracks your code, they won’t be able to meet the second verification requirement, which immediately blocks their access to your accounts. Other benefits of this double step include:

* Reducing cyber vulnerability
* Removing password and username risks
* Boosting online security
* Improving cyber hygiene

This layered security approach, combined with a complex password, can protect your online purchases, bank accounts, and identity from potential hackers. The extra step is crucial to minimizing attacks and enhancing your digital experience.

Other security tips to follow

Being vigilant in cybersecurity efforts is essential to thwart online cyber-attacks. It’s up to you to make it harder for hackers to crack your code. Keep your accounts secure by reading [a guide to cybersecurity hygiene,](https://digital.va.gov/cyber-spot/your-guide-to-better-cyber-hygiene/) or by following these tips:

* Always use multi-factor authentication as an additional layer of protection.
* Ensure passwords have a minimum of 12 characters. Create a custom acronym.
* Do not use passwords compromised in security breaches.
* If a site provides a temporary password, immediately change it after logging in.
* Never share your passwords.

Cybersecurity works when you do!

When incorporated with complex passwords, multi-factor authentication can be the barrier between hackers and your accounts. An increasing number of services we rely upon are managed online through websites or mobile applications. Creating unique passwords and implementing multi-factor authentication when prompted gives you cyber peace of mind knowing bad actors must work harder to crack your code.