



**WE ARE
BEING
DOXXED:
WHAT TO DO TO HELP
KEEP EACH OTHER SAFE**

The alt-right has gotten hold of some of our online accounts. With this information they are creating imposter accounts in order to harass, phish, and dox us. They are sharing our personal photos along with addresses and phone numbers to encourage further harassment. Their efforts have been far reaching and are expanding. Now is a crucial time for us to take our data security seriously and review our practices. We particularly encourage those of us who may feel off the radar to examine security practices, as we have seen a willingness to target less visible or publicly active friends both for harassment and for information mining. Individual security is about keeping all of us safe.

No tool can save you from your behavior. We emphasize good practices over encouraging use of apps and programs. The internet is an incredibly volatile place and it's important we have a critical and suspicious eye when thinking about how we exist online. We encourage you to walk through your online presence as an adversary, see what could be exploitable. Take steps to protect yourself from anyone gaining access or control of your accounts, but first weigh the risks of having your data compromised versus the utility its online access gives you. We've resisted and existed for centuries without the technology currently used, make sure only things you want to be online are online.

This is not meant to be wholly comprehensive. Lots of this advice will not protect you from adversaries that have wide-spread access and advanced tools. We suggest you address these immediate concerns, yet continue to strengthen your digital self-defense.

FOR AN EXTENDED LIST OF RESOURCES AND GUIDES ON HOW TO IMPLEMENT SOME OF THE PRACTICES RECOMMENDED, CHECK OUT:

[DIGITALDEFENSE.NOBLOGS.ORG](https://digitaldefense.noblogs.org)



LOOK OUT FOR PATTERNS

If something doesn't feel right, take the time to figure it out. Take the time to verify identities. There are many ways to do this, in person being by far the best, but talking with your voices on the phone or a short face-time/video-call can be used to confirm the identity of who you're interacting with. Be critical when people get new numbers or contact you from accounts you're not familiar with (our forgotten old accounts can sometimes be revived by an attacker). We've seen attackers simulate crisis in order to get information quickly. We've seen attackers overstate when attempting to gain trust, your friends aren't often going to list five reasons they are themselves (especially when a quick call will do). If something isn't comfortable, don't do it.

SCRUTINY

Attackers have many ways of gaining access to your accounts and information. Often times they'll hide malware inside a seemingly innocuous link. As good practice, don't click on links but type in the address instead. Don't be curious without making sure you're safe. When browsing websites, sensitive information could be leaked just by visiting. There are plenty of tools out there to help you; using the TOR browser or a VPN (such as Private Internet Access) can assist you with some aspects of your security, but take some time to learn their limitations. If you have a tech-savvy friend, ask them to attempt to dox you in order to patch holes in your security.

Visit ssd.eff.org and explore their interactive website. More than anything, take your online presence seriously. No one is perfectly secure, but we can all be patching the holes in our collective security. This current iteration of threats is about our connections to each other, so even if you don't feel you're an at risk person one small weak spot makes a huge mess for all of us. Be critical and scrutinize. **Trust, but verify.**

HERE'S A SHORT LIST OF ACTIONS YOU CAN DO TO PROTECT YOURSELF FROM SOME OF THE EXACT PROBLEMS WE'VE RECENTLY FACED. IT REALLY MATTERS.

- GET OFF SOCIAL MEDIA IF YOU CAN. IF NOT, KEEP OUR FACES OFF OF IT.
- DON'T LET ACCOUNTS LINGER. LOCK DOWN ANY ACCOUNT YOU OWN, OR MAKE SURE THEY'RE DELETED IN THOROUGH AND SAFE WAY.
- DON'T RE-USE PASSWORDS. USE A SIX WORD PASSPHRASE AT A MINIMUM FOR EACH ACCOUNT.
- KNOW THAT YOUR SMARTPHONES ARE CONSTANTLY COLLECTING YOUR DATA AND SYNCING IT TO THE CLOUD AND/OR GOOGLE DRIVE.
- KEEP YOUR ACCOUNTS CLEAN OF CONTACTS, PHOTOS AND OLD EMAILS. ONLY HAVE THINGS ONLINE THAT YOU NEED TO HAVE ONLINE.
- ERR ON THE SIDE OF CAUTION. ASK FOR VOICE OR VIDEO CONFIRMATION IF DEALING WITH A CONFUSING OR SUSPICIOUS CONTACT.



SOCIAL MEDIA

As our adversaries learn our identities and map our relationships we've seen an increasing amount of impersonations and "phishing" (attempts at luring people into giving more information). One way to start our defense is to limit the access to mapping in the first place. Take a critical eye to your social media accounts and make them private. Look at who you're following and who's following you. Verify new accounts, as many fake accounts are created to monitor or impersonate your friends and comrades. If you know of a fake or harassing account, document it and report it. Take down identifying pictures and be thoughtful of the social web you're advertising. If you choose to delete any account, learn about how it may be recovered, as our attackers have reactivated and thereby controlled accounts. Think back to every online account you've had, go back and lock them down with secure passphrases and two-factor authentication (when possible).

GOOGLE, ACCOUNTS AND EMAIL

With a few notable exceptions, your accounts are collecting and storing large amounts of information on you. These accounts allow you some say on what and how this is stored, and it's highly suggested you personalize your account to be relevant to your concerns. For instance, Android phones sync your contacts with Google/Gmail to make everything more accessible to you. If someone were to gain access to your account and therefore contacts, they could learn names, numbers, and emails for people they could be interested in as well as a list of people to try to harass, hack, or phish for other information. With enough opportunities and practice there stands a good chance that someone could get the information they need or cause the damage they desire.

Delete all the information you weigh as risky, and be critical. Your archive of emails is a treasure trove of personal information, delete all the emails you don't need to hold on to. If you want to keep some, but don't want them to be accessible from your account, get them offline (print them, to PDF or paper). Remember, most services just move items to a Trash folder when you delete them, make sure to clear it. Look at your recovery

options. Security questions can be easily guessed depending on how much information someone has on you; make your answers nonsensical passphrases or don't use security questions at all. Don't let everything rest on a central account, this provides an option where if an attacker gains access to one of your accounts they can gain access to many (Google allows you to log into everything with one account, you can see how risky this would be once an attacker gains access to that one account). "Forget your password" and see what vulnerabilities exist to someone attempting to get yours.

PASSPHRASES

Currently the recommended advice is to have a passphrase of at least six randomly selected words in sequence. While a shorter passphrase with symbols and seemingly random characters is very hard to remember, it's not an effective barrier to most programs that are used to crack passphrases. If remembering decent passphrases for all your accounts seems daunting, consider using a password manager (like KeePassXC). Don't re-use passphrases, an account with low security using the same passphrase as say, your online banking, creates an obvious and easily exploitable breach in security. Change them frequently, set time aside to re-up your security with regularity. When applicable use two-factor authentication/verification and opt for methods that aren't easily bypassed (such as choosing to use an offline app over sending a text to a phone i.e. Google Authenticator).

<https://ssd.eff.org/en/module/animated-overview-how-make-super-secure-password-using-dice>

RECORD EVERYTHING

So much of data is ephemeral, especially if you lose access to your accounts. Print (to PDF) emails or screenshot conversations you consider suspicious. The same goes for if you're contacted by a potential attacker. These instances can serve as examples of things to look out for, and could come in handy if you need evidence to get an account shut down, pursue a lawsuit, or regain control of your account.