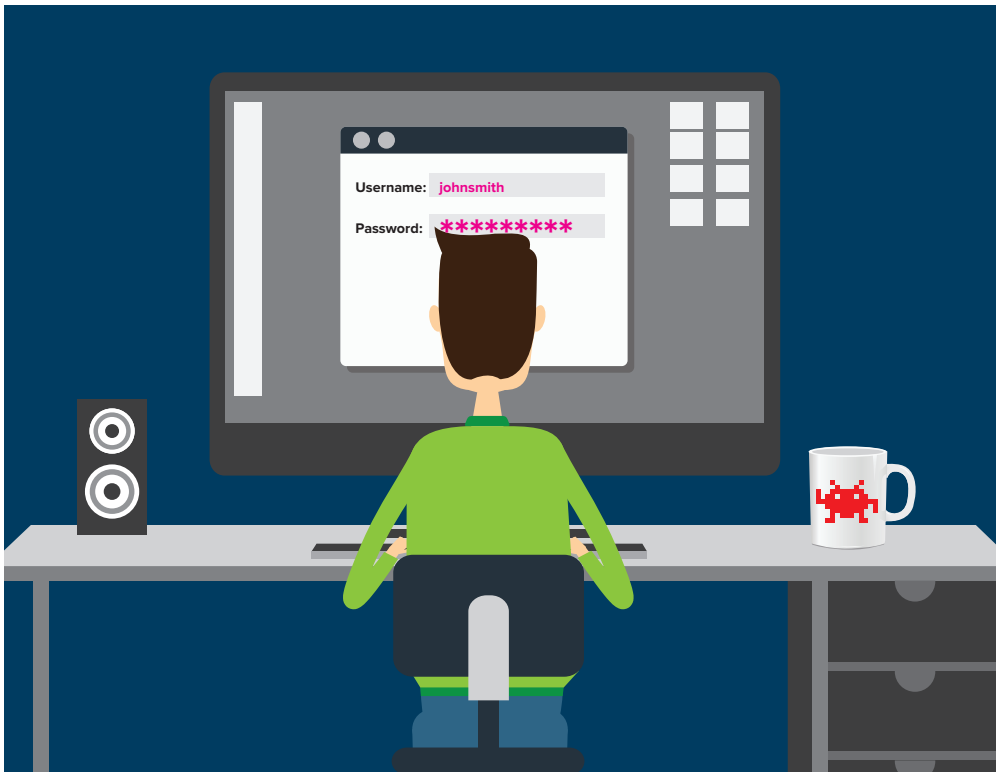
UpGuard™

HANDBOOK

9 Steps for Optimum Password Security

The Password Security Checklist



OVERVIEW

You might have read about Facebook founder and user Mark Zuckerberg's social media accounts getting "hacked." Hacked is maybe not the right word here, since many people believe Zuck's password was among the 117 million leaked LinkedIn passwords recently posted online. If this is true, it means that Zuckerberg used the same password for multiple websites, allowing the damage done by the LinkedIn hack to spread into other areas. If you have or want a job, chances are you also have a LinkedIn account, and if you had one back in 2012, it was probably one of the compromised accounts from that incident. Do you still use that password anywhere? Our 9 step password security checklist will help you secure your accounts, whether you're a billionaire CEO or just someone who likes to post funny cat videos.

1. NEVER SHARE YOUR PASSWORD WITH ANYONE. SERIOUSLY.

The very first thing you're going to want to do, if it wasn't part of your OS setup, is change the root password. This should be self-evident, but can be surprisingly overlooked during a routine server setup. The password should be at least 8 characters, using a combination of upper and lowercase letters, numbers and symbols. You should also set up a password policy that specifies aging, locking, history and complexity requirements if you are going to use local accounts. In most cases you should disable the root user entirely and create non-privileged user accounts with sudo access for those who require elevated rights.

- Tech support
- Cops
- Your friend who is actually really cool
- A judge
- Mom
- Someone asking for it in an email
- Your boss
- Famous hacker Kevin Mitnick
- Literally anyone

Your password is what makes you accountable for the actions taken under your account. Socially engineering a password out of someone is often much easier than "hacking" their account. Most *ishing schemes trick you into giving up your password in some way or another. Why go to the trouble of blowing the safe if you can have the bank manager open it up for you?

2. CREATE A STRONG PASSWORD

Not just any password will do, and the reason why relates to how passwords are cracked. If a person were trying to guess your password, they might try ten or so passwords a minute, if they're fast. A computer can guess much, much faster. So how many permutations does it take to get your password? Here are three key factors:

- Length. Each character increases the complexity exponentially. This is why passwords typically have a minimum requirement of 8 characters.
- Character sets. Each character set has a certain number of permutations. There are 26 lowercase letters, but only 10 digits (0-9), so you can see how "potato" is more secure than "536871" from the perspective of a machine running through different combinations of characters.
- Common words. Brute force isn't the only method to crack a password. A computer can run a "dictionary attack" against a password very quickly, testing for all real words, of which there are relatively few, compared to the huge number of character permutations possible. All of the sudden "potato" isn't that great of a password after all.

Your password should be a combination of at least both upper and lowercase letters and a number (62 unique, reusable characters, with 8 characters in the password means 62 to the 8th power, or 2.1834011e+14 possible combinations...) Include a special character to increase complexity, but make sure that character is supported by the mechanism you're using, as some are not. Finally, you can find any number of password generators online, which can generate extremely complex passwords. But you have to remember this. And when you get down to step 5, having separate passwords for every account can be too much to ask with 18 character randomly generated passwords.

3. SET A REMINDER TO CHANGE YOUR PASSWORD

Some services require regular password changes, while some do not. If they don't, it's always a good plan to change your password regularly anyway. This step is about reducing the window of damage. Going back to Zuck, if his password was obtained in 2012, it has no business still being in use in 2016. A simple reminder every six months or even a year would have prevented this old data breach from compromising anything. The more often you change your password, the smaller the window of a compromised password being worthwhile. This is why high security systems use randomly generated numbers that change every few minutes as part of their authentication model. Changing your password on a regular basis may seem annoying, but it's nothing compared to dealing with a compromised account, identity theft, or credit card fraud.

4. DON'T REUSE PASSWORDS

Alternating between passwords doesn't have the same effect as changing them to something new each time. Once a password is compromised, it can be exploited at any point in time, even years later, as Zuckerberg found out. Reusing a password re-opens the vulnerability window for that password.

5. DIFFERENT SITES? DIFFERENT PASSWORDS.

This is the one Zuck really got nailed on. Limiting the scope of your password prevents a compromised password from exploiting multiple areas. Even adding a section somewhere in your password like "fb" for Facebook (eg: BuFFDuD3fb) will prevent most cross-site compromises, because once the attacker realizes the same password won't crack the site, they would then have to manually start guessing at differences, without knowing if it's an entirely different password altogether. The full effect of the LinkedIn data breach has likely not been seen yet. As email/password combos are tried at other sites, users who relied on a single, static password will be compromised. This ripple effect to other systems follows major breaches every time.

6. SECURE YOUR RESET OPTIONS

This step protects you against people, rather than computers, trying to hack your account. Be thoughtful with how your password can be reset. Security questions and answers should not be information that is publicly available, easily searchable or widely known to people who know you. Many people's accounts are hacked by people they know in real life. If you have an email account where a password reset request will be sent, make sure you have sole access to that account and that it too has a strong password.

7. PASSWORD MANAGERS

You can use a password manager to store your passwords for you. The major browsers all have password storage systems, while cloud options like LastPass work from any computer with internet access. There are pros and cons to this method:

Pros	Cons
Don't have to remember all the passwords.	For browser managers that automatically log you in, it means if your laptop is stolen, so is access to all of your accounts.
No really, it's a lot of passwords to remember.	Single point of compromise for multiple systems.
More time to not remember passwords.	Passwords in the hands of a third party.

Consider that LastPass suffered a data breach in 2015 where sensitive information was acquired by hackers. The encrypted master password was not compromised, but much other important information was. The important thing to remember is that password managers are not magic-- you're simply outsourcing the protection of your passwords to someone else.

8. USE TWO-FACTOR AUTHENTICATION WHENEVER POSSIBLE

The one account of Zuckerberg's that didn't get breached was his Instagram, and that's because "Instagram's security systems prevented that account from being accessed." This could refer to a few things, but likely means the two-factor authentication (2FA) Instagram set up in February of this year.

Probably one of the most important mechanisms available, 2FA, as its name implies, prevents the compromise of a single authentication factor (the password) from compromising the account. The mechanism typically works by requesting the traditional login information, then sending a confirmation to a device, usually a smartphone, such as a text, phone call, or in-app security verification screen. Ideally, only the authorized person would have the smartphone and could then accept or reject the authentication requests as necessary. More advanced mechanisms can require bio-authentication, such as a fingerprint swipe, which prevents lost or stolen phones from being used to falsely issue confirmations. Most cloud apps offer 2FA now, with many traditional applications following suit. It's worth taking a few extra seconds every time you login to know that even if your password is hacked, nobody can access your accounts.

9. DON'T LEAVE ANY OPEN WINDOWS

There's a classic cartoon gag where one of the characters struggles for a long time to pick a lock on a door while the other character just goes in through an open window. Don't let this be the case with your data. Consider whether there are other accounts with access to the same information you're protecting. Are they as secure as yours? What about integrations? Did you try out that hilarious face swapping app that requested access to your Twitter and Facebook and photos? Does it still have access to your account? Most cloud services will let you track what third party integrations have access and remove whatever is unnecessary. If you're using a public computer, be sure to close the entire browser process when you're done. Failure to do so could leave your session cookies available for the next person, who wouldn't even need to log in to access your information.

CONCLUSION

Digital identity management is in that weird place between new enough that many people don't bother with it, and established enough that sophisticated attacks seek to exploit it. A username and password may seem like just a bit of data you toss into the cloud whenever, but the consequences of compromise are very real, and can be legal, financial and personal. Or they can be funny, like when the official NFL Twitter account was hacked to make greatly exaggerated claims of Roger Goodell's death.According to the hackers, they "got the NFL's Twitter password by hacking the email account of an employee who handles social media." Take care of your password like you would your driver's license or debit card. Following the steps we've outlined here will help protect you against the most common types of account hacks, but security is a habit, and keeping it in the forefront of your mind when using the internet will always pay off.