



Our guide to password management for accountants

Passwords are a necessary evil in your increasingly digital accounting world, and unfortunately, a weak password is a golden ticket for cybercriminals seeking to exploit sensitive financial data.

While the internet is full of advice and guidance on creating robust passwords, the sheer volume of often-contradictory guidance from various regulatory bodies, industry associations and online forums can be incredibly confusing, making it difficult to determine best practices. The National Cyber Security Centre (NCSC) offers clear guidance, advocating for the 'three random words' strategy, which aims to keep sophisticated hackers out while ensuring you can still remember your crucial passwords and access client data and financial systems.

As accountants, you rely on passwords daily to access a multitude of critical platforms: accounting software, banking portals, tax filing systems, client management databases and a host of other applications containing highly confidential information.

In this guide, you'll find best practices exploring password management for accountants, and you'll learn about the most commonly made mistakes to avoid, helping you safeguard your firm's and your clients' financial integrity.

Passwords: the fundamentals

A password, for an accountant, is a confidential word, expression, or string of characters used to prove your right to access critical financial data, client files and sensitive accounting software.

As the world has continued its shift to a more digital way of working, the requirements for creating new passwords have significantly escalated. What began as a simple word or phrase has evolved, and you're now typically required to include a complex mix of upper and lower case letters, numbers, special characters and adhere to a minimum character count.

Some systems, particularly those handling highly sensitive financial information, even mandate regular password changes or prevent you from reusing previously used combinations, all in an attempt to mitigate the chance of a data breach. However, it's important to note that the National Cyber Security Centre (NCSC) and other leading cybersecurity bodies now generally discourage frequent mandatory password changes, as this can actually lead to weaker password habits.

It is almost certain that you already use numerous passwords as part of your daily accounting routine, whether that's to log into your firm's email, access online banking for client accounts, or manage cloud-based accounting platforms. However, sometimes a single, reused password is the only thing protecting all of your valuable client data and proprietary business information. It's easy to fall into the trap of choosing the same combination for multiple accounts.

Unfortunately, this poses a problem as when more and more accounts are created, it becomes difficult to choose different passwords and remember which combination matches which account. If one of these widely used passwords is compromised, a cybercriminal could gain access to a vast amount of your professional and client data.

Ultimately, it is your choice as to which passwords you use and how you manage them. When implemented correctly, strong, unique passwords are a free, easy, and incredibly effective way to prevent unauthorised individuals from accessing your personal or business financial information, protecting both your accountancy's reputation and your clients' security.

Common password mistakes and trends

Cybersecurity firms and news outlets consistently highlight the alarming prevalence of weak passwords, a critical vulnerability that poses a significant threat to accounting firms handling vast amounts of sensitive client data. For the accountancy sector, a data breach can lead to severe financial penalties, reputational damage, loss of client trust and even regulatory investigations.

The most commonly used passwords worldwide in 2023, and the frequency of use, are as follows:

- 123456 – 4,524,867
- Admin – 4,008,850
- 12345678 – 1,371,152
- 123456789 – 1,213,047
- 1234 – 986,811
- 12345 – 728,414
- Password – 710,321
- 123 – 528,086
- Aa123456 – 319,725
- 1234567890 – 302,709

It's clear from these findings that a large majority of the online population, which will likely include professionals within the accountancy sector, are falling into the same habits of copying, repeating or using generic, easy-to-remember passwords. This makes your firm and your clients' sensitive financial data extremely easy targets for cybercriminals. Robust password management for accountants must be a top priority, starting with a strategy that moves beyond these easily compromised patterns.

What to avoid when creating a new password

- Password reuse: trying to remember passwords can be hard and this leads to many people using the same password on many, if not all, accounts. While this makes it easy to remember, it also makes it easier for the cybercriminal. If they crack your password for one account, they consequently have access to all of your accounts.
- Using personal information: many passwords include pet names, children's names, birthdays and dates of birth. It is not difficult to guess this information or search the internet, including social media profiles, to get it.
- Default passwords: some websites fail to change the manufacturer's default device passwords or worse the default password is easy to guess, for example, 'admin' or 'password'.
- Letter replacements: swapping letters for special characters and numbers is still very common practice and this is one of the first things hackers will test when trying to gain access to your accounts.
- Passwords from patterns: they can look complex at first glance, but if they are the top row of a keyboard or a sequence of any kind they become easy to predict and break.

Types of possible password breaches

Effective password management for accountants is crucial for protecting the highly sensitive financial and personal data you handle daily. Cybercriminals employ a variety of sophisticated techniques to breach security, and understanding these methods is your first line of defence.

Here's a breakdown of common password breach techniques that accounting firms must be vigilant about:

- Dictionary attacks: These are a fundamental form of brute-force attack where hackers use automated programs to rapidly test your password against extensive lists of common words, phrases, and previously exposed passwords. For accountants, this means that using terms related to your firm, industry, or even common financial jargon can make your passwords vulnerable. Combining seemingly random letters, numbers, and special characters significantly increases your resistance to these attacks.
- Phishing attacks: Cybercriminals are increasingly using sophisticated social engineering scams to trick you into voluntarily supplying login credentials and other confidential information. This is often conducted through highly convincing fake emails, text messages, or cloned websites that mimic legitimate entities like HMRC, client portals, banking institutions,

or even internal IT support. AI-powered phishing is making these attacks even more realistic and personalised. Comprehensive training for all staff is absolutely essential to prevent your accountancy firm from falling victim.

- Password spraying: Unlike repeatedly attempting different passwords on a single account (which can trigger security alerts), this technique involves using a few widely used passwords and trying them across a large number of usernames.
- Credential stuffing attacks: This tactic involves cybercriminals using login details (username and password) stolen from one data breach to try and access your other accounts. If your credentials from a less secure site are compromised, attackers will then use those exact same combinations to try and log into your more critical accounting software, banking portals, or client management systems.
- Vulnerable website exploitation: In these attacks, cybercriminals target an accountancy website or service with weak security that your firm uses. Their goal is to steal your credentials from that site, which they can then leverage for further, more damaging attacks against your firm's systems and sensitive financial data.

How secure is your accountancy's passwords?

There are websites available where you can check your current passwords to see how secure they are or if they have been compromised online. Please take care with any site offering this service, as you will be sharing your password and do not use it if it is asking for your email address for a password to be checked.

How to ensure a secure password choice

- Below, we've outlined essential best practices to keep in mind, whether you're creating a new password for an accounting system or upgrading an existing one:
- Use a minimum of 12 characters (this is the Net-Defence policy) longer is better but you need to balance this with remembering it
- Ensure the words are random and have no association with you, your family, pets, or hobbies
- Make sure you use different passwords for different accounts
- Make sure they are easy to remember but are hard to guess (three random words is a good strategy e.g. PencilSpatulaGorilla)
- Don't write down any passwords, try and make them easy to remember
- Never tell anyone your password (make sure you are the only one accessing your accounts)
- Make sure your software and devices are kept up to date
- Be vigilant towards other people trying to see your passwords (e.g. over your shoulder, recording on a smartphone)

By consistently implementing diverse and robust passwords, you significantly reduce the risk of a widespread data breach, helping to safeguard your clients' financial integrity and your firm's professional reputation.

Password storage options

Utilising an encrypted password vault or manager is an effective strategy to centralise and safeguard your multitude of credentials. These tools provide a secure, categorised repository for your passwords, mitigating the risk of forgetting individual logins.

However, it's vital to choose a strong, unique master password for the vault itself, as losing access to it could mean losing access to all your stored information.

Many reputable options are available, ranging from free versions to more feature-rich paid subscriptions. Here are some common and recommended categories:

Net-Defence

Ogilvie House, Princes Park, Team Valley Trading Estate, Gateshead NE11 0NF • Ogilvie House, 200 Glasgow Road, Stirling FK7 5ES
Tel: 03300 241 666 • Web: net-defence.com

- Internet browser: this is a secure option as long as the browser remains updated (security updates applied), and the account has a strong password.
- Smartphone: similar to the internet browser option, this will remain secure as long as iOS and other operating updates are applied, and the device has password functionality turned on (PIN – 6 or greater, facial recognition, fingerprint access).
- Application: N-able's Pass portal is a reputable and recommended application that stores your passwords. Be sure to research, taking reviews into account, and choose an option that you deem to be safe and reliable.

Where does Net-Defence come in

For accountancy firms navigating the complex digital landscape, cybersecurity is a fundamental aspect of risk management and client trust. While we at Net-Defence cannot dictate your specific password choices for compliance, we are dedicated to empowering you with the knowledge and tools necessary to make informed decisions about robust password management for accountants.

We offer tailored training sessions, delivered directly within your firm's workplace. These sessions educate your accounting team on the latest threat landscapes, focusing on how to identify and defend against sophisticated phishing attempts, ransomware, and other forms of data breach attacks that frequently target the financial sector. This proactive approach strengthens your human firewall, often the weakest link in cybersecurity.

Furthermore, we provide in-depth Cyber Resilience support specifically designed for accounting practices. Our services include thorough Penetration and Vulnerability testing, where our ethical hackers scan your network, accounting software and digital infrastructure for potential weaknesses. We then work collaboratively with you to develop and implement effective solutions to patch these vulnerabilities, ensuring your firm remains secure and compliant amidst evolving cyber threats.

To fortify your overall cybersecurity strategy and protect your clients' sensitive financial information, visit our website or [get in touch](#) with our team of specialists today.