THE TECH CHRONICLE

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

HOW TO SAFELY SHARE PASSWORDS WITH EMPLOYEES

If you ask a security professional, you get by-the-book advice about sharing passwords: "Don't share passwords." But we know, in reality, that doesn't work. Your office might be sharing a single password for apps like SurveyMonkey right now to save cash on buying additional users, and some social media accounts don't even give you the option to have multiple log-ins.

Sharing passwords in your office is sometimes necessary for collaboration, and the best way to do this is by using a password manager. Affordable (some platforms even offer free versions), layered with security and simple to use, password managers are the safest and easiest way to store and share your company's private passwords.

Reasons You Would Need To Share Your Passwords

Share accounts are the biggest reason businesses share passwords, whether their employees work from a physical office or at home. It improves collaboration and makes employees' jobs a lot easier.

Medical leaves, turnover, vacations and "Bob isn't coming in because he ate bad fish last night but has our Amazon log-in" are other reasons passwords get handed around like a plate of turkey at Thanksgiving dinner.

However, unsafe sharing habits will put your private passwords in the hands of greedy hackers, who can fetch a high price for your data in dark web markets. IBM Security reported that in 2022, 19% of all breaches were caused by stolen or compromised credentials.

So, how do you share passwords safely?

First, Avoid These Common Password-Sharing Mistakes

When it comes to password sharing, remember:

continued on page 2...

WHAT'S NEW

We will have a new ticket submission system coming online in the next few months! Not much will change on the client side - you'll still have an icon on your desktop where you can submit a request for support and include details and screen shots of the relevant information.

This new system will allow us to increase efficiencies and prioritize critical requests. We'll be sending out additional information when we get closer to the transition time with instructions, expectations, etc in order to make the change over as seamless as possible!

This monthly publication is provided courtesy of Craig Covington co-owner of Canon Capital Technologies.

OUR MISSION:

To enhance our customer's quality of life and the health of their businesses.

...continued from cover

> IBM Security reported that in 2022, 19% of all breaches were caused by stolen or compromised credentials.

- Don't send passwords via e-mail: E-mail is the #1 target of hackers, and many e-mail services aren't encrypted. Those that are encrypted are still risky because e-mails are stored in several servers on their way to or from your account. That means your e-mail is sitting in a Sent folder, ripe for the taking by anyone who gets into your e-mail account, encrypted or not.
- Never text or chat passwords: Like e-mails, SMS messages or messaging apps like Slack aren't secure. Once a text is sent, it's available for anyone to see.
- Stay away from storing passwords using pen and paper and shared documents: Sticky notes, memo pads, Google Docs – NEVER write down your passwords.
- Avoid the temptation to store passwords on your device: If your device gets hacked, nothing stops that perp from taking every password you saved.

The Best Way To SAFELY Share And Store Your Passwords

We recommend using reliable password managers because they have multiple layers of encryption so only those with a key (your master password) can see it, AND they include more robust security and sharing features like:

- Zero-knowledge architecture: Not even your password manager service can see the information you save in your vault.
- Multifactor authentication (MFA): For added log-in security.
- Unique password generation: Creates strong, random passwords to improve log-in security.
- Fake log-in page warnings: Warns you if a page is spoofed by hackers.
- Breach or weak password notification: Alerts you if one of your passwords was leaked or if your current password is weak.
- Simple, secure built-in password sharing: Some password managers let you choose which passwords your employees can see and keep others in a private vault. Others, like Keeper, let you share documents or records without exposing credentials.

To use password managers, you only need to remember one password – the master password. One downside is that whomever you share a password with needs an account for the same service. However, most password managers have corporate accounts, so this shouldn't be a problem.

A Word To The Wise: Look out for password managers with a bad security track record, like LastPass, which was breached in 2022, 2021, 2016 and 2015.

Smart Businesses Use Password Managers

It's a good idea to avoid sharing passwords as much as possible, but when you have to, use a reliable password manager to ensure you have control over exactly who sees your credentials. Talk to your employees about safe password hygiene, host regular security-awareness training for employees and use MFA with every account. It's not just safe business – it's smart business.

If you're not sure which password manager to use, give us a call and we'll get you set up with one.

WHAT IS CONFIDENCE?

Confidence is a fundamental trait in the world of business. You may think all the great CEOs and entrepreneurs of the last few decades have never lost their confidence, but you'd be wrong. New CEOs usually have impostor syndrome and struggle with the idea that they're good enough for their role. Self-made billionaires worry that their fortune will take an embarrassing hit. Even private equity investors look at the looming recession and grow concerned.

We often find leaders are less confident when they obsess about things out of their control rather than take action in areas where they have some control. The Wall Street Journal recently reported that most CEOs are externally most worried about a recession, global trade and politics. Internally, they're much more concerned about retaining top talent, avoiding disruptive technologies and developing the next generation of leaders. While it's good to be aware of the external issues, it's much more important to master the internal problems within your control.

In order to fully boost your confidence, you must have a high level of confidence in your team. If you are already confident in your team, keep doing what you're doing to hire and develop top talent. If you aren't confident in them, then you should work on hiring the right people. If you've found yourself in this position and are simply not confident enough in your team, you can do a few things to remedy the situation.

Your first option is to invest your own time into hiring, training and developing your team yourself. You need to set ample time aside to truly master the necessary skills to see the best results. Additionally, you can hire a company like ghSMART to do it for you. We can devise options for an immediate fix that will help adjust your confidence while building your team's skills.

Confidence is not necessarily an inherent trait we get from our genes. We can build and grow our confidence skills by managing the things within our control. There will always be uncontrollable outside pressures, and there's simply nothing we can do about it. Instead, focus on hiring and maintaining top talent, developing your company's digital capabilities and training the next generation of leaders. You'll see positive results before you know it.

Dr. Geoff Smart is the chairman and founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times bestsellers. He stays active in his community and has advised many government officials.

ADAPT WITH THE CHANGES

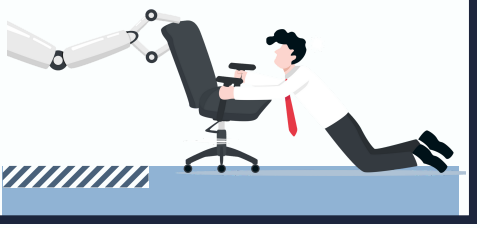
To Reach Continued Success

The economy is constantly evolving, and your business needs to adapt with it if you hope to stay relevant. Currently, our economy is in a strange state due to recently coming out of a pandemic, and many economic experts believe we're teetering on the edge of a recession.

If you want to see success in the coming years, you need to focus on these two areas.

Hiring: Don't let location stop you from hiring the best talent for each open position. Hire remote and hybrid employees if they are the best fit for the job.

Artificial Intelligence (AI): AI isn't going anywhere, so becoming familiar with it now will help you develop an advantage over your competition.



CARTOON OF THE MONTH