TECH TIPS

TECHNOLOGY INSIGHT THAT BUILDS BUSINESS

HODGSON CONSULTING & SOLUTIONS

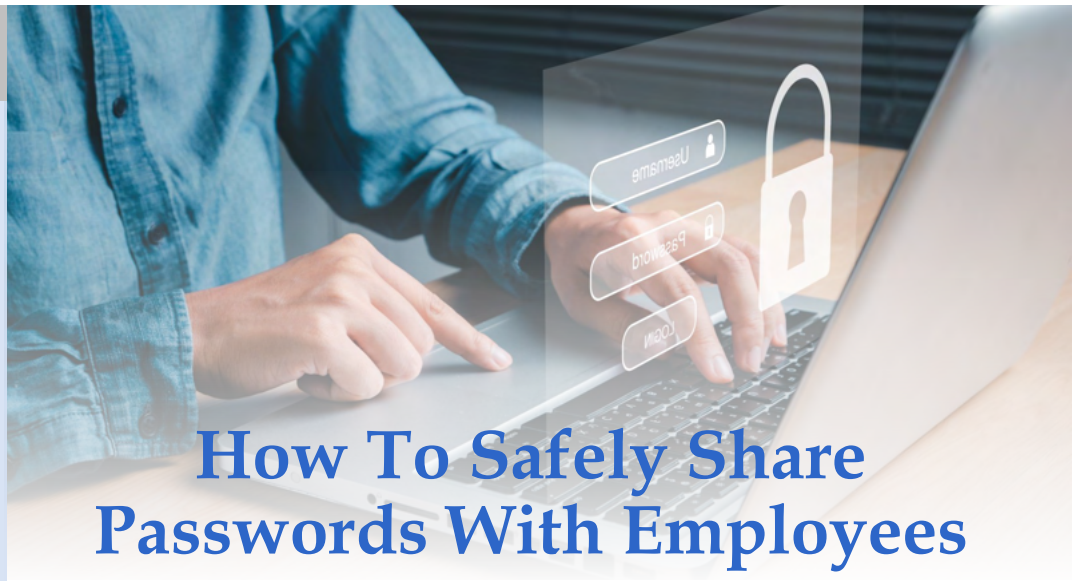
Inside This Issue

September 2023

This monthly publication is provided courtesy of Robert Zehnder President of Hodgson Consulting & Solutions.

Our Mission:

To eliminate every technical frustration, obstacle and inefficiency for companies with multiple locations and/or a remote workforce.



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

Shared 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:

1. **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.
2. **Never text or chat passwords:** Like

Continued on pg.2

Continued from pg.1

emails, Like e-mails, SMS messages, or messaging apps like Slack aren't secure. Once a text is sent, it is available for anyone to see.

3. **Stay far away from storing passwords using pen and paper and shared documents:** Sticky notes, memo pads, or Google Docs – NEVER write down your passwords.
4. **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.

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

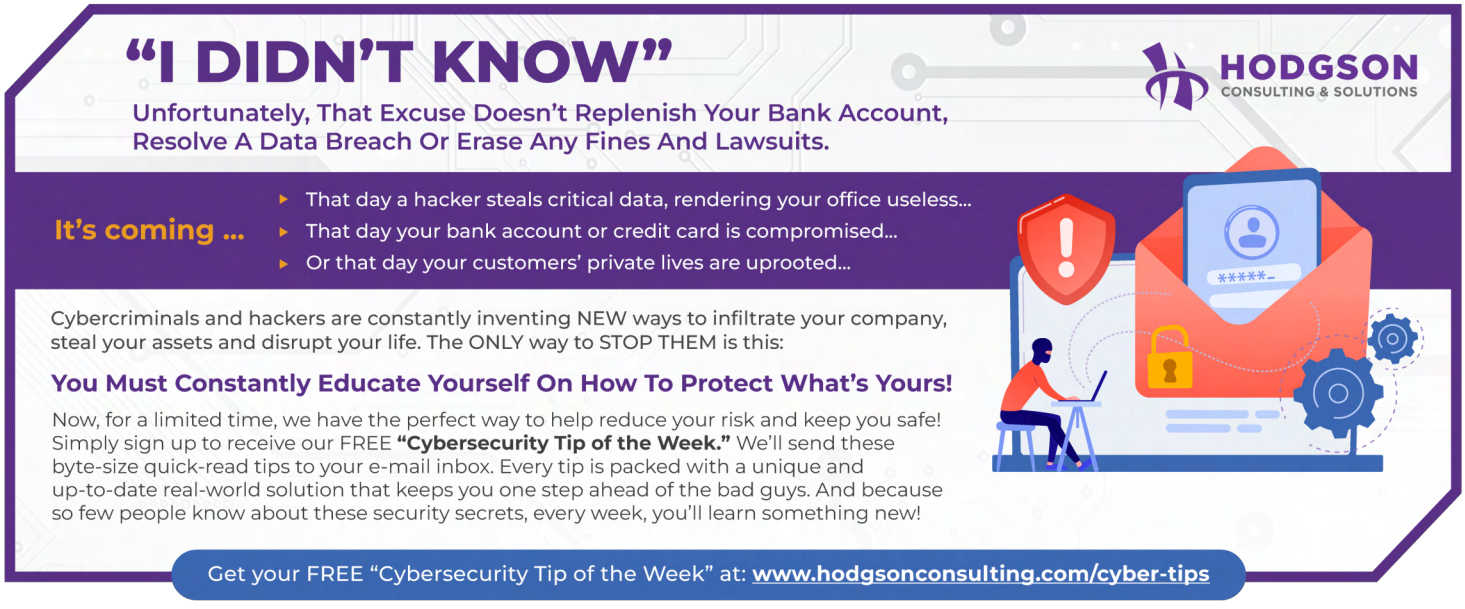
To use password managers, you only need to remember one password – the master password. One downside is that whomever you share a password with needs an account for the same service. However, most password managers have corporate accounts, so this shouldn't be a problem.

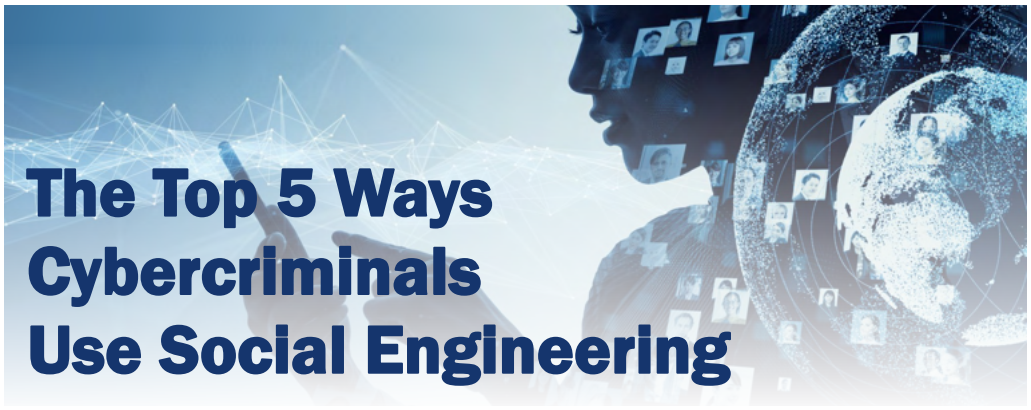
A Word To The Wise: Look out for password managers with a bad security track record, like LastPass, which was breached in 2022, 2021, 2016, and 2015.

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.





The Top 5 Ways Cybercriminals Use Social Engineering

People often say that innovative technology and hacking techniques are how cybercriminals attack victims online. But did you know hackers can also use a less complicated way to get people to trust them online? It is a time-honored method of manipulating others by winning their trust and taking advantage of their emotions, known as cyberattacks for social engineering.

Common Methods of Social Engineering Attacks

Social engineers employ many inventive strategies to carry out their cunning plans. There are five distinct ways hackers use cyberattacks for social engineering to their benefit, listed here:

Phishing

Phishing is by far the most common and most effective tactic that cybercriminals use in social engineering. It has been around for years, yet people continue to fall for it at an alarmingly high rate. Emails are the most popular method used for phishing. Anyone with an email account has probably seen several phishing attempts in their inbox.

Some of the first phishing emails came from a Nigerian prince who said he would give you a big chunk of his money if you helped him get his inheritance. Phishing emails have gotten cleverer over time, such as fake emails that appear to be from your bank and ask you to confirm your account number. Social media phishing has become more common in recent years, especially in cyberattacks using social engineering. One trick is when they ask you to enter your account information on a fake social media site that looks real.

Baiting

A social engineering technique called baiting involves dangling something in front of the target victim, hoping they will click on a link and fall into the trap. It's usually something the victim would want, like free music or a movie. Of course, the link does not provide them with what they promised; instead, it contains malware that harms your computer or network.

Pretexting

In this social engineering scam, the hacker contacts the victim by pretending to be someone the victim knows. They might act like the head of IT doing an inspection and ask an employee for their login information. Or they could act like a law enforcement official or an investigator to steal private information. If the employee thinks a hacker is a trusted person, they might not think twice about giving away their login information.

Quid Pro Quo

This is a type of social engineering attack where the hacker offers you something in exchange for critical information. Let's say a disgruntled employee has been laid off or has left a company on not-so-amiable terms. Hackers hunt down these disgruntled individuals and offer to buy the information that they can use to attack the company.

Piggybacking

Although most cyberattacks using social engineering take place online, there are many tricks used in a physical setting. One such instance is piggybacking. Tailgating, or "piggybacking," is when someone sneaks behind an authorized worker into a closed-off part of the building. Once inside, they can quickly gain access to computers and steal data.

There are so many ways that cybercriminals use social engineering for malicious intent these days. However, there are also several things that you can do to keep safe from these attacks. Many of the preventive measures are actually very simple, starting with never revealing passwords and other sensitive data to anyone. This includes heads of IT departments, people in charge of corporate audits, or even law enforcers.

As a business owner, it is also crucial to ensure that you educate all your employees fully when it comes to social engineering attacks and other cybercrimes. We have plenty of tools and resources that can help boost your protection against all kinds of cyberattacks.

Experience Fewer Errors With New Hires

By Refining Your Onboarding Process

Onboarding is an essential part of the hiring process. While interviewing allows you to select the right person for your open position, onboarding gives you an opportunity to train them before they start their day-to-day responsibilities. This is your chance to set them up for success. If you haven't already done so, document the tasks for every position in your company in the coming weeks. Speak with the person currently in that role to ensure you don't miss any critical functions. This will give you a great start to a flawless onboarding system. From there, you can document any questions or concerns that arise in future onboarding sessions to cover any holes. With time, your onboarding process will soon run itself!

Want To Become A Better Leader?

Learn How To Manage Yourself First

Every business owner and leader wants to lead and inspire their team effectively, but this is easier said than done. You're going to face challenges within your business that will put your mettle to the test. Many of these obstacles will stem from your team as you learn to manage different personalities and overcome communication barriers.

If you want to lead your team properly, you must take a step back and focus on yourself first.

Many employees look to their leaders for support, encouragement, and guidance. As their leader, you have to remember you are setting an example for your team, so you must stay aware of every action you take. Pay attention to how you talk to people and how you're spending your time while at work. You should be acting in the same manner you would expect from every other member of your team. If you're not, it's time to make some adjustments. Your business's success and your employees' behavior begin and end with you. Become the leader you would want to work for, and your employees will respond positively.

Is It Time For A Vacation From Work?

Business leaders want their companies to be profitable and often dedicate hours of overtime every week to ensure everything runs smoothly. While this might give your business a boost, it can be damaging to your mental health. Many leaders have a hard time taking a break from their business and end up burning out before reaching the pinnacle of success. Don't fall into this trap. Here are a few warning signs to pay attention to that tell you it's time to take a break from work.

You feel anxious or nauseous every morning before work. Your body will tell you when it needs a break. Listen to it!

You make careless mistakes. Overworking ourselves can take away from our focus, which causes us to make mistakes we wouldn't normally make.

Your motivation has vanished. If you feel like you have to force yourself through the motions at work, it's likely time for a vacation.