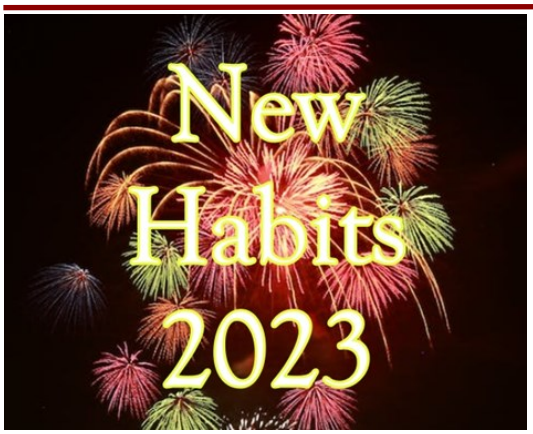
ACT SMART I.T.
Helping You Benefit From Today's Technologies

January 2023 BUSINESS EDITION

Top 10 Resolutions for 2023



Around the New Year, people usually get ready by making a list of things they need to work on based on what they have learned in the past year.
The same thing is true for cybersecurity. By building on what has been learned over the past year, we can get better at defending ourselves against new threats.

We have come up with a list of resolutions that don't require you to join a gym or cut down on sugar (even though we all should do it anyway).
Our suggestions are some steps you can take to improve your cyber readiness and make your digital life safer.

1. ***Think before you click*** - Cyber-criminals often use current news, sensational topics, and promises of shocking photos and videos to get you to click on malicious links. Don't fall for it!
   Stop and think before you click.

2. ***Change your passwords*** to pass ***phrases***
   A. Make your password hard to guess
   B. Give each of your online accounts a unique password
   C. Do not use your own information as a password. Don't use your name, birthday, address, or even the name of a pet as a password.

3. ***Protect your privacy*** - As Consumers, We Must Take Responsibility For Our Own Privacy Settings. Helpful links on our website...

4. ***Implement multi-factor authentication*** where possible (https://staysafeonline.org/online-safety-privacy-basics/multi-factor-authentication/)

5. ***Choose security over convenience –***
   A. When asked to save your credit card information on a shopping website– DON'T. If that company is breached, they have your credit card information as well as other vital facts about you!
   B. Don't save your password to your browser! Cyber criminals know to look in Chrome or Firefox to look for your list of saved passwords!

6. ***Embrace Cybersecurity Awareness and Training –*** 80% of all ransomware attacks and data breaches are caused by human error. Simple and effective training can be the best defense.
   A. Make it a point to keep up-to-date about cybersecurity – 80% of all ransomware and data breaches are caused by human error. Continual training reminds of the dangers and can be simple as well as effective.

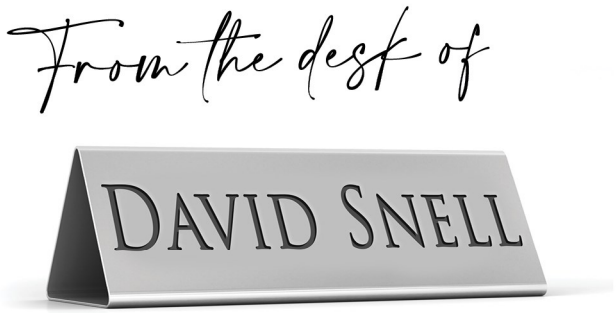
7. ***Avoid Oversharing Your Personal Information***
   What you share online can give thieves clues to your passwords, your routines and your life!

8. ***Keep Your Devices Up To Date*** – updates and patches often contain the most up-to-date security developments. Don't leave the back door open for cybercriminals

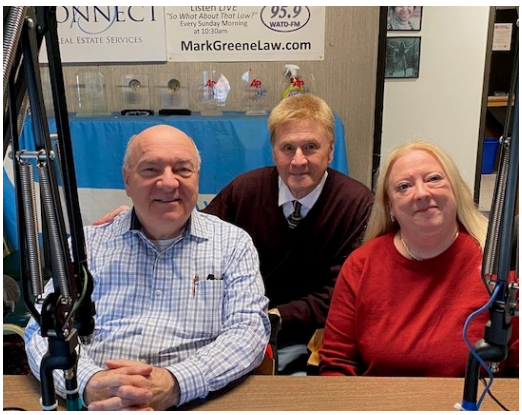
9. ***Backup Your Essential Data*** – Use the 3-2-1 backup rule
   3 = Create one primary backup and two copies of your data.
   2 = Save your backups to two different types of media.
   1 = Keep at least one backup file offsite.

10. ***Use a password manager*** to make it easy to have the unique and secure passwords that you need today. Many are FREE for individual use.
    For a business-grade password manager – contact us and we'll help you find the one that's best for your business or practice.

For more information and links to helpful sites, go to ACTSmartIT.com/2023-2



As I finish writing this newsletter, our most pressing challenge is password manager LastPass's breach and the resulting probable exposure of our personal, most sensitive information. We DO NOT use LastPass for our business; it's the password manager that Pam and I use to keep and share our passwords for everything personal.



We're spreading the word because you may also use LastPass as your personal password manager. Pam and I have recommended it for years, including most recently on Attorney Mark Greene's "So What About That Law?" radio show January 1st on 95.9 WATD.

If you use LastPass, we recommend that you change all your passwords ASAP. Although we understand this is a monumental undertaking, you'll need to take action right away. Start with the most valuable passwords like Amazon accounts where you will most likely have a credit card linked to your account, banking accounts, mortgage companies, insurance companies and any logins with information that an attacker could use for identity theft.

We strongly recommend that you also enable 2FA (2 factor authentication) on every account that offers it. This is the best way to protect yourself and your passwords in the future.

You can find more information and can listen to his Tech Talk radio spot on 95.9 WATD on page 5 or visit: https://actsmartit.com/lastpass-password-vaults-stolen-by-cyber-criminals/. You can also click on **David's Blog** at the top of our home page for a link to that and all his blog posts.

Data Privacy Week
2023 CHAMPION

Other news: we are calling 2023 "The Year of Videos" here at ACTSmart. We'll be having monthly webinars and other informative videos throughout the year. We've swapped out one of the offices so that we can record them in a little peace. You're less likely to hear the fire engines and ambulances go by from this recording spot.

We're happy to announce that we are once again ***Data Privacy Week Champions.*** We've participated since the beginnings of Data Privacy Day. We think that Data Privacy should be maintained every day of the year!

To help you keep control of your data privacy, StaySafeOnline.org has created a very handy page with links to the most popular sites and apps's Privacy Pages. You simply click on the links and adjust your settings to your preferences. As they point out, does your solitaire game really need to know your location and contacts?

Take a few moments to read our front page article "Ten Resolutions for 2023." They may be a little easier to keep than giving up sugar and will just as good for you and your well-being!

Our mantra is: Choose Security Over Convenience!

Data Privacy Week is January 22—28, 2023

ALL YOUR ONLINE ACTIVITY GENERATES A TRAIL OF DATA.

Websites, apps, and services collect data on your behaviors, interests, and purchases. Sometimes, this includes personal data, like your Social Security and driver's license numbers. It can even include data about your physical self, like health data – think about how a smartwatch counts and records how many steps you take.

While it's true that you cannot control how each byte of data about you and your family is shared and processed, you are not helpless! In many cases, you can control how you share your data with a few simple steps. Remember, your data is precious, and you deserve to be selective about who you share it with!

Here are some simple, easy tips you that will help you manage your data privacy:

Know the tradeoff between privacy and convenience

Nowadays, when you download a new app, open a new online account, or join a new social media platform, you will often be asked for access to your personal information before you can even use it! This data might include your geographic location, contacts, and photos.

For these businesses, this personal information about you is tremendously value — and you should think about if the service you get in return is worth the data you must hand over, even if the service is free.

Make informed decisions about sharing your data with businesses or services:

- Is the service, app, or game worth the amount or type of personal data they want in return?
- Can you control your data privacy and still use the service?
- Is the data requested even relevant for the app or service (that is, "why does a Solitaire game need to know all my contacts")?
- If you haven't used an app, service, or account in several months, is it worth keeping around knowing that it might be collecting and sharing your data?

Adjust privacy settings to your comfort level

For every app, account, or device, check the privacy and security settings. These should be easy to find in a Settings section and should take a few moments to change. Set them to your comfort level for personal information sharing; generally, we think it's wise to lean on the side of sharing less data, not more.

You don't have to do this for every account at once, start small and over time you'll make a habit of adjusting all your settings to your comfort. We have in-depth, free resources like Stay Safe Online **Manage Your Privacy Settings page (https://staysafeonline.org/resources/manage-your-privacy-settings/)** that lets you check the settings of social media accounts, retail stores, apps and more.

Protect your data

Data privacy and data security go hand-in-hand. Along with managing your data privacy settings, follow some simple cybersecurity tips to keep it safe. We recommend following the Core 4:

- Create long (at least 12 characters), unique passwords for each account and device. Use a password manager to store each password – maintaining dozens of passwords securely is now easier than ever.
- Turn on multifactor authentication (MFA) wherever it is permitted – this keeps your data safe even if your password is compromised.
- Turn on automatic device, software, and browser updates, or make ure you install updates as soon as they are available.
- Learn how to identify phishing messages, which can be sent as emails, texts, or direct messages.

Thanks to: https://staysafeonline.org/programs/data-privacy-week/individuals/ for this critical information

Proactive Retention

Tis the season!! It is the time of year when people start to think about what is next for their career; are they living their best life, are the relationships genuine, simply put, do they LOVE their job and what they do? So, it begs the question, what can we do as HR professionals and leaders to proactively retain and engage our people? Let's take a pulse on some info we are hearing....

Did you know over 70% of US turnover is preventable?

Since March 2020, companies across the globe have been analyzing the effects of remote or hybrid work models. Focusing on where an employee works may be diluting other factors: nine out of ten individuals want flexibility over when they work. In "The Great Executive - Employee Disconnect," Slack reported that employees feel 2.4x better about their work-related stress when having flexibility. But when provided with schedule flexibility, that number increases to 6.6x. What does a flexible working arrangement mean for your team? As we approach 2023, it's clear that remote work does not always mean flexibility.

The *New York Times* published a shocking podcast in August 2022, revealing that eight of the ten largest private US employers track the productivity metrics of individual workers in real-time. Salaried workers are starting to echo complaints that employees in many lower-paid positions have voiced for years: their jobs do not allow for autonomy or any control of their own. Tracking impressions is not fool-proof; check out a "mouse jiggler," for example. Companies were reported taking screenshots of their staff every ten minutes during billable hours. Others have started deducting pay for idle time or lack of digital impressions - even in client-facing fields. Beyond compliance concerns, this type of behavior is not sustainable. Focus on trust-building touchpoints and strategic supervision.

Maybe you've heard the term "quiet quitting" from LinkedIn. In response, the Harvard Business Review (HBR) published "Quiet Quitting Is About Bad Bosses, Not Bad Employees." HBR's team concluded that trust, after analyzing data from 100,000+ leaders, trust was the most important factor. Leaders should strive to adopt the following behaviors to empower their teams and build trust:

1. **Maintain positive relationships** with all of your direct reports. Are you engaged with your team's individualities? Common interests bind you together, while differences are stimulating. Look for and discover common ground with these team members to build mutual trust.

2. Beyond transparency, **leaders need to deliver on what they promise.** Most leaders believe they are more consistent than others perceive them. Following through on your commitments, regardless of how small, builds confidence amongst your team.

3. **The third element that builds trust is expertise**. Do you know your job well? Do others trust your opinions and your advice? Clear insight builds confidence in your expertise.

For example, if someone is meeting their deliverables and has the capacity, assign them a high-priority responsibility, empowering them to grow within the organization. If a different team

SteinbergHR is a woman-owned human resources boutique consulting firm providing engagements that are interim, part-time, and project-based. Reach out to Meghan Steinberg, Founder of SteinbergHR, to talk through your goals for this upcoming year and explore the possibilities for 2023 to re-engage and re-energize your organization that aligns with your strategy.

Let's connect: Meghan@steinberghr.com or call 617-680-0358.

For Positive Outcomes

member is struggling, reflect on their strengths and weaknesses - and come up with a plan to scale up their skillset. When taking action, try to avoid comparing employees - it's proven that diverse teams are the most successful. *Forbes* concludes, "As a manager, building trust is all about your ability to look through the crisis, challenge, or situation and see the person standing before you."

Think of your people's strategy like lightbulbs. Do you replace the incandescent bulb or invest in LED? The savings will not be reflected on your next invoice, but within a year, you will save 75% more energy, and that bulb will last 25 times longer. Being proactive now will save your company valuable resources: be bold when finalizing your 2023 budget. Invest in flexibility. Invest in trust. Invest in your people.

This article is brought to you by SteinbergHR; created and edited by Maddie Thomas and Meghan Steinberg, referencing various articles, data points, and perspectives. Please read in more depth the resources.

Meghan Steinberg, PHR, SHRM-CP is the Founder and President of SteinbergHR, LLC. She has an operations background with solid HR foundations and experience coupled with HR certifications and creativity. Her firm supports an array of businesses of all industries, from start-ups, family and Fortune 1000 companies.

Maddie Thomas is a Senior HR Generalist. Her quest and specialty is strengthening people's strategies to support optimal business practices within global operations.

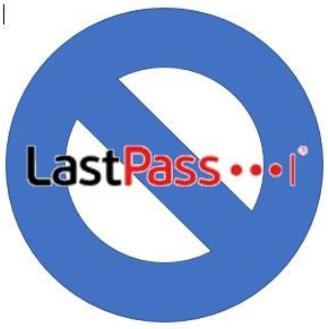
Sources:

https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html

https://hbr.org/2022/08/quiet-quitting-is-about-bad-bosses-not-bad-employees

https://www.forbes.com/sites/theyec/2022/05/18/nine-smart-and-effective-ways-to-build-trust-with-your-employees/?sh=541cb2a85bc8

https://www.bls.gov/news.release/tenure.t03.htm



LastPass Password Manager Breach

We finally know the extent of the LastPass breach and it is not a good situation. The breach was disclosed back in August 2022 by LastPass when they told their users that an unauthorized party got into some development servers and stole source code and some LastPass technical information.

Fast forward to the end of November, LastPass stated information obtained during that earlier compromise had enabled a threat actor to access "certain elements" of customer data within a third-party cloud storage service. Again, it was stressed that customer passwords remained "safely encrypted."

In the December 22 update, LastPass explains how the threat actor was able to "access and decrypt some storage volumes" from the cloud-based storage service, physically separate from the LastPass production environment. The problem is that this cloud-based storage service stored backups, including entire backups of customer vault data.

In his statement, LastPass CEO Karim Toubba states that encrypted fields in the stolen data vault can only be decrypted using the "unique encryption key derived from each user's master password." The fact that a cyber-

Continued on page 7

Things are Changing in the Cybersecurity

Cyber Insurance, or Cyber liability Insurance as it's called, has become an ever-evolving market. It covered everything from data processing errors and online scams to malware infections when it first appeared.

The increase in online danger and rising costs of a breach have led to changes in this type of insurance. In today's environment, no one is safe, not even the small family-run bakery. Insurance companies know that small businesses often have fewer security protocols in place than larger enterprises, and they

have more to lose. It's important to review your cyber insurance policy at least once a year and ensure you know what is covered and excluded.

Here are a few areas to ask your insurance agent if your policy covers:

- Recovering compromised data – via ransomware such as Cryptolocker
- Repairing computer systems in the case of ransomware
- Costs associated with notifying customers about a data breach – mailouts,
- credit monitoring, etc.
- IT forensics costs to investigate a breach
- Legal expenses concerning client lawsuits over the breach
- Expenses for the downtime while forensics is researching – employee costs, lost revenue, etc.
- Ransomware payments – hopefully, you're using our backup services, so you won't have to pay the ransom ~ but if you're not, will they pay the bad guys for your data?

This list isn't exhaustive; it's the baseline of questions to which you should know the answer regarding your cyber insurance policy.

And you may want to ask, "If I have an incident, how

long do I have to wait for you to "investigate" before I can restore my backup or do whatever it takes to get back to work?" If your agent says they can't provide an exact time frame, ask them to give you a ball park estimate based on other claims they've seen processed. Someone there has that answer.

Here are a few things to keep in mind this year regarding Cyber Insurance.

Demand is Going Up

The average cost of a data breach is currently $4.35 million (global average). In the U.S., it's more than double that, at $9.44 million. As these costs continue to balloon, so does the demand for cybersecurity insurance. Companies of all types realize that cyber insurance is critical and as vital as their business liability insurance.

Premiums are Increasing

With the increase in cyberattacks has come an increase in insurance payouts. Insurance companies are increasing premiums to keep up.

In 2021, cyber insurance premiums rose by a staggering 74%. Insurance carriers aren't willing to lose money on cybersecurity policies.

Certain Coverages are Being Dropped

Certain types of coverage are getting more difficult to find. For example, some insurance carriers are dropping coverage for "nation-state" attacks. These are attacks that come from a government, and many governments have ties to known hack-

Insurance Market - Are You Prepared?

ing groups. So, a ransomware attack that hits consumers and businesses can very well be in this category.

In 2021, 21% of nation-state attacks targeted consumers, and 79% targeted enterprises. You may want to ask your agent what information they use to classify cybercriminals as "nation-state" actors. Another type of attack payout that is being dropped from some policies is ransomware. Insurance carriers are tired of unsecured clients relying on them to pay the ransom. So many are excluding ransomware payouts from policies, which puts a bigger burden on businesses.

It's Getting Harder to Qualify

Unlike every other insurance, just because you want cybersecurity insurance doesn't mean you'll qualify for it, and if you do, the premium may be outrageous. Insurance carriers aren't willing to take chances, especially on companies with poor cyber hygiene (lack of security protocols).

Here are some of the factors that insurance carriers are looking at:

- Network security
- Use of things like multi-factor authentication or biometrics
- BYOD (how many employees are using their own devices) and device security policies
- Advanced threat protection
- Automated security processes
- Backup and recovery strategy
- Anti-phishing tactics
- Employee security training
- Physical security

With the new year just starting, now would be a great time to review your current cyber insurance policy and how your business aligns with your coverage.

LastPass Breach *Continued from page 5*

criminal has an entire backup copy of LastPass' password database file, it's only a matter of time before they break the encryption and begin their attacks.

Based on this information, it is our very strong recommendation that every LastPass user immediately log into every account for which you have a saved password in LastPass and change that password.

Although I understand this is a monumental undertaking, you'll need to take action right away. Start with the most valuable passwords like Amazon accounts where you will most likely have a credit card linked to your account, banking accounts, mortgage companies, insurance companies and any logins with information that an attacker could use for identity theft.

I strongly recommend that you also enable 2FA (2 factor authentication) on every account that offers it. This is the best way to protect yourself and your passwords in the future.

Do you need to quit LastPass?

Whether you think LastPass is a service you can continue to trust or not is for you to decide. The transparency in companies declaring breaches is always to be applauded, although many questions remain as to why it has taken LastPass so long (almost 4 months) to determine and disclose that actual password vaults had been stolen. Based on this information, I will no longer recommend LastPass as a secure password vault.

No company can be 100% safe from breaches; that's a simple truth, but trust is paramount in the world of password management, and there can be little doubt that this trust has been broken for LastPass users. ACTSmart has a password management solution (PassPortal) that you can move to. PassPortal is the application we use for managing our clients secure passwords. Pam and I have been using LastPass for years for our personal use and are moving to PassPortal.

Give David a call if you're interested. 781-826-9665

ACTSmart IT
332 Main Street
Wareham, MA 02571

In This Issue

Know a business who could use this type of information? Send them to ***ACTSmartIT.com/newsletters***

OFFICE MANAGERS SOCIETY

Tuesdays at 8:11 am on 95.9 WATD fm

95.9 FM WATD
THE SOUTH SHORE'S RADIO STATION

Did you know that David has been on The South Shore's Morning News with Rob Hakala for over 20 years?

On most Tuesday mornings, he and Rob have ***Tech Talk*** about trending tech information including what Microsoft, Apple, Google, Metaverse (Formerly know as Facebook) and other companies are up to.

One of the topics this month was the LastPass password manager's breach which concerns us greatly! You can read more about it on page 5. If you are a LastPass user like we were, it's an article that you can't miss!

He posts these topics on his blog and, if you weren't able to catch his radio spot, you can hear it on our website or, have it delivered to your inbox!

ACTSmartIT.com/blog-2