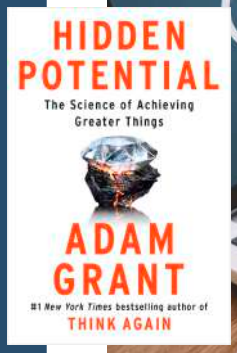
WCI Technology Insider

Insider Tech Tips - Written for Humans, Not Geeks

Hidden Potential: The Science of Achieving Greater Things

by Adam Grant



Hidden Potential offers a new framework for raising aspirations and exceeding expectations. Adam Grant weaves together groundbreaking evidence, surprising insights, and vivid storytelling that takes us from the classroom to the boardroom, the playground to the Olympics, and underground to outer space. He shows that progress depends less on how hard you work than how well you learn. Growth is not about the genius you possess - it's about the character you develop. Grant explores how to build the character skills and motivational structures to realize our own potential, and how to design systems that create opportunities for those who have been underrated and overlooked.

**source: adamgrant.net/book/hidden-potential*

September 2024

Bill Wright
Founder & CEO

Our Mission:
Technology systems that anchor your business and protect what you have built, from a company inspired to make the world better.

Slow PCs?

Manage which applications launch at startup

Staying on top of how your technology is set is crucial for maintaining a reliable network. And one often-overlooked aspect is managing which applications start up when your business's PCs start up.

With lots of software wanting to auto-start, it can slow down your system and potentially introduce security risks. But, did you know that Windows 11 offers a useful feature that alerts you whenever new apps are added to the startup list?

Every time you hit the power button on you PC, it loads a set of apps automatically. While some are essential, others might not be, and can slow down your system's performance. Over time, as you install more software, your startup list can grow, leading to longer startup times and a slow experience.

Not only that, but keeping an eye on startup apps is a good security practice. Unwanted or unknown apps starting automatically can be a red flag for malicious software (malware) or other security threats. By receiving alerts about new startup apps, you can quickly identify and investigate any suspicious additions, making sure that your systems stay secure.

How do you enable these alerts in Windows 11?

It's a simple process:

- Start by opening the Windows 11 system settings. You can do this by clicking the 'Start' menu and selecting the gear icon, or by pressing 'Windows + I' on your keyboard.

Continued on Page 2 ...

... Continued from Cover

- In the settings window, click on 'System' in the left sidebar, then select 'Notifications' on the right.

- Scroll down to the bottom of the notifications page. Just above "Additional Settings", you'll find 'Startup App Notification', which is switched off by default. Move the slider to 'On'.

From then on, you'll receive a notification whenever a new application is added to the startup process. You can even customize what this notification looks like by clicking on the arrow next to the slider button, allowing you to adjust its appearance and sound to suit your preferences.

Turning on these alerts brings several benefits to your business. First, it helps to keep your PCs running efficiently. By staying informed about new startup apps, you can quickly disable any unnecessary software that might be slowing down your system. This means faster start times and better overall performance, allowing your team to get to work without delays.

Secondly, it enhances security. Receiving alerts for new startup apps means you can immediately investigate any unknown or suspicious additions. This proactive approach helps prevent potential security threats from taking hold, safeguarding your business data and systems.

Lastly, it's a great way to keep track of what's installed on your machines. With various team members possibly installing different software, these alerts give you a clear overview of what's being added to the startup list, making sure that only approved applications are running.

To further manage startup apps, you can use Task Manager. Press 'Ctrl + Shift + Esc' to open Task Manager, then select the 'Startup' tab. Here, you'll see a list of all the apps that start with Windows, along with their impact on boot time. You can enable or disable apps by selecting them and clicking the appropriate button at the top right.

By regularly checking this list and using this new alert feature, you can keep your startup process streamlined and your system secure.

A better answer is getting someone to set all of this up and manage it for you. We specialize in making technology easy for businesses. If we can help, get in touch.

Byte-Sized Quiz

In an attempt to protect proprietary data and day-to-day workplace online activity, many companies utilize a VPN for employees, which provides a secure connection to a different network than public Wi-Fi. What does the acronym VPN stand for?

A. Verified Personal Network

B. Virtual Private Network

C. Virtual Protected Network

Answer: B. Virtual Private Network

What We've Been Chatting About This Month

Regular cyber security training gives your business the highest level of protection

Want to join the conversation? Our new guide is up on our website multimedia page, under 'monthly guides' now!

TECH FACTS

#1

In 2002, Welsh website llanfairpwllgwyngyllgogerychwymdrobwllllantysiligogogogoch.co.uk won the title for the longest website URL in the world. It lost the title in 2006, when 6 other people registered longer URLs, but in 2007, the Welsh URL was upgraded from 63 to 68 characters and regained its title.

#2

The first computer password is believed to have been created in 1960s, by Fernando Corbato, who worked on the Compatible Time-Sharing System (CTSS) at MIT. He created it so that several people could share the computer he built.

#3

The microwave oven was an accidental invention. A researcher, Percy Spencer, discovered that every time he walked past a cavity magnetron tube the chocolate bar in his pocket melted.

Bill's Favorite Business Gadget of the Month

Flexispot Electric Standing Desk

We all know that sitting down all day is no good for us, but when you have an office job, it's unavoidable. Or is it?

The Flexispot Electric Standing Desk lets you stand while you work, making it easier to move around and giving your posture a boost, too.
It has a silent motor, is quick to assemble, and has a digital keypad that allows you to add height presets (including a sitting position, of course).

Starting at $239.99 on Amazon

Inspirational Quote of the Month:

"Transparency within your organization is the difference between having a business that's simply running and having one that's moving in one direction."

-Michael Riedijk, CEO of PageFreezer Software

The WCI Team's Favorite Everyday Gadget of the Month:

Anker Prime 20K Power Bank

Remarkably, the Prime 20K Power Bank by Anker can charge two laptops via a pair of fast USB-C connectors with a maximum power output of 140 watts. It has a battery pack with ample capacity and, rather impressively, a color screen to help you keep tabs on the charging process. The accessory rocks a USB-A connector, so you can simultaneously charge up to three devices.

Check it out today!

There's a cyber threat you might not have heard of

There's a cyber threat you might not have heard of - Account Takeover (ATO) attacks.

It's when cyber criminals gain unauthorized access to your online accounts. This can expose sensitive data, enable financial theft, and allow further attacks. And it's happening more than you might think - ATO attempts skyrocketed by 427% last year.

Cyber criminals use sophisticated techniques to steal your login details, often using generative AI. This AI can create incredibly realistic phishing emails that appear to be from someone you trust, tricking even the savviest people into giving up their details. It's what's making the attacks so dangerous.

Imagine a cyber criminal gains access to the email of a senior person in your business. They can send fraudulent messages to employees, partners, or clients. And it's not just a hypothetical scenario - 75% of businesses reported at least one ATO attack last year, and more than a third faced more than five incidents.

So, how do you protect your business? Here's my advice.

Encourage employees to use complex passwords generated randomly and stored in a password manager.

Use Multi-Factor Authentication where you get a login code on another device. It's not foolproof, but it adds an extra layer of security.

Invest in advanced security tools that can detect unusual activities and potential threats.

Give your team regular training on recognizing and avoiding cyber threats.

Remember, being proactive is always your best defense. If my team can be proactive for you, get in touch today.

https://www.techradar.com/pro/mitigating-the-growing-threats-of-account-takeover-attacks-in-2024

Is it time to be *more like Alex?*

Here's a story about a business owner named Alex. Alex runs a successful marketing agency, and business has been booming. But with growth comes growing pains, and Alex has found himself increasingly bogged down by IT issues.

At first, Alex tried to handle everything himself. After all, he was pretty good with computers. And for a while it seemed to work. Alex managed to fix minor issues and keep things running.

But then, one Monday morning, disaster struck. Malicious software had infected the company's main server, crippling their operations. Alex spent days trying to fix the issue, losing valuable time and money in the process. It was a wake-up call: Doing it himself wasn't a sustainable solution.

Determined to avoid another disaster, Alex decided to train his top employee, Sarah, to handle IT alongside her regular duties. Sarah was smart and quick to learn, but the additional responsibilities quickly became overwhelming. She found herself too thin, and her productivity in her main role started to suffer. Not to mention, the fast-paced tech world was hard to keep up with, and soon, Sarah felt like she was drowning in a sea of updates and security threats.

Realizing this wasn't working, Alex considered hiring an in-house IT team. But the costs were daunting. Recruiting skilled professionals, providing ongoing training, and equipping them with the right tools would require a significant investment. For a mid-sized business, this was a heavy financial burden.

That's when Alex discovered the benefits of outsourcing IT. He found a reputable IT service provider with a team of experts, ready to step in.

Here's what Alex found:

1. **Expertise on tap:** The outsourced IT team brought knowledge and experience. They were always up to date with the latest technologies and security threats, making sure the agency's systems were secure and efficient.

2. **Cost savings:** Instead of paying salaries and benefits for a full-time team, Alex paid a monthly fee based on the services he needed. This was a much more affordable solution.

3. **Focus on core business:** With IT taken care of, Alex and Sarah could focus on what they did best - growing the business. Productivity soared, and so did their client satisfaction.

4. **Scalability:** As the agency continued to grow, the outsourced IT team easily scaled their services to meet the increasing demands. No need for Alex to worry about hiring more staff, or buying new equipment.

Alex's story is a great example of why outsourcing IT is a smart move. It frees up time and resources, allowing you to focus on what you do best, while experts handle the complexities of IT.

If you want to take a page from Alex's book, get in touch.

Did You Know

Cyber extortion has increased by 108%?

Cyber extortion is when cyber criminals threaten to damage, steal, or expose a business's digital data unless a ransom is paid. **And the number of victims has grown 77% year on year.**

In the US, attacks have risen by 108% **and any business of any size is targeted.**

To stay better protected, the usual advice applies: Make sure all software is up to date, back up your data, and implement multi-factor authentication (where you get a code on another device to prove it's you).

New to Microsoft

Excel on the web has a revamped look

Microsoft is giving Excel on the web a face lift. It has new features that make it faster to add and resize rows and columns, rearrange elements with drag and drop, to highlight critical information, and to improve readability.

The Excel app for Windows and Mac has also got new features, such as checkboxes and support for OpenDocument format.

Cyber Security *is a team effort*

There are loads of important things you need to think about for your business. Loads. But we're adding another one to your list: cyber security awareness.

You'd be forgiven for thinking this is an IT problem; something for them to sort out. But, we're sorry to say it - you're wrong. It's something that every single person in your company needs to be on top of, from the big boss to the latest hire.

You see, cyber threats are always changing and getting more sophisticated. A one-time training just won't cut it. You need to keep everyone in the loop with regular updates. Think of it like this - in the same way you need regular check-ups to stay healthy, your team needs regular cyber security training to keep your business safe.

What does this training look like? There are a couple of ways to do it. First, there's the good old traditional method - you know, lectures and presentations. One way of training. These are great for laying down the basics and introducing new concepts. But, let's be honest, they can be a bit... boring.

That's why it's a great idea to mix in some interactive training, too. Imagine phishing simulations where your team learns to spot fake emails before clicking on them. Or hands-on workshops where they can use the security tools and protocols they're been hearing about. These methods are not only more engaging, but also help the info stick better.

Combining these traditional and interactive methods is where the magic happens. Start with some solid grounding through presentations, and then get everyone involved with practical exercises. This way, the knowledge isn't just in one ear and out the other - it's learned, remembered, and applied.

Let's talk frequency. Since cyber threats are always evolving, training shouldn't be a once-a-year thing. Regular sessions throughout the year will keep your team sharp and ready to handle anything that comes their way.

Creating a strong cyber security culture in your company is key. This means making cyber security everyone's responsibility. Encourage a culture where if someone spots something fishy, they speak up right away. Communication is super important here.

And remember, this starts at the top. If the leaders in your company are taking cyber security seriously, everyone else will, too. So make sure the big shots are not only participating in the training, but also showing how important it is. Lead by example, right?

Cyber security is something that affects the whole business. Every email, link, and password matters. By making sure everyone is trained and aware, you're building a strong first line of defense against cyber threats.

We can help you get your team started - just get in touch.

Technology Update

Average ransomware demands are soaring

Cyber criminals are getting confident. And they're asking for obscene ransoms to give you back your data after ransomware attack (that's where they lock or encrypt your computer files and demand payment to unlock or decrypt them).

The average demand in the first half of this year? **More than $5 Million.** It's time to get the right security measures in place.

let's go back to school
with this month's fun tech quiz

1. **What language is used most on the internet worldwide?**
2. **How many apps are in the Apple Store?**
3. **What's the official name for the "prove you're not a robot" test?**
4. **What does URL stand for?**
5. **What was the first emoticon ever used?**

The answers are on page 8.

Question: Should I let my employees use company apps on their personal phones?

Answer: Ideally not, because you have less control over the security of personal devices. If htey need to work on a phone, it's better to provide a company-issued one.

Question: Should I ban my team from working in coffee shops because of public Wi-Fi dangers?

Answer: You don't have to. Just make sure they're aware of the risks of using public Wi-Fi and that they're vigilant when connecting to new networks.

Question: Should we delete phishing emails, or should they be reported?

Answer: Any spam or phishing emails should be flagged as such becuase it teaches your email provider what spam looks like. You can also forward it to the Federal Trade Commission (reportphishing@apwg.org)

QUIZ Answers

1. ENGLISH
2. ALMOST 2 MILLION
3. CAPTCHA. IT'S AN ACRONYM FOR 'COMPLETELY AUTOMATED PUBLIC TURING TEST TO TELL COMPUTERS AND HUMANS APART.
4. UNIFORM RESOURCE LOCATOR
5. :-) IN 1982 BY COMPUTER SCIENTIST SCOTT FAHLMAN. EMOTICONS ARE MADE UP OF KEYBOARD CHARACTERS, WHEREAS EMOJIS ARE LITTLE PICTURES.

WCI TECHNOLOGY SOLUTIONS

81 Mill Street, Suite 300
Gahanna, OH 43230

@WCITech

WCI Technology Solutions

@WCITech

Human or Robot?

Am I the only one who's spent way too much time overthinking those squiggly letters, street sign puzzles, or "click all the buses" pictures on websites?

Those "prove you're not a robot" tests are called CAPTCHA.

That Stands for "Completely Automated Public Turing test to tell Computers and Humans Apart."

Phew, that's a mouthful!

Simply put, it's a tool designed to differentiate between bots and real humans.

CAPTCHA was invented in the early 2000s by a group of clever people at Carnegie Mellon University. They realized that, as the internet grew, so did the number of bots trying to cause chaos.

Their solution? A test that humans can easily pass, but bots struggle with. And thus, CAPTCHA was born.

Fun Fact: CAPTCHA has evolved into reCAPTCHA, a tool from Google that often involves identifying objects in pictures. Not only does it keep your site safe, but it also helps train AI by identifying things like street signs and house numbers. Pretty cool, right?