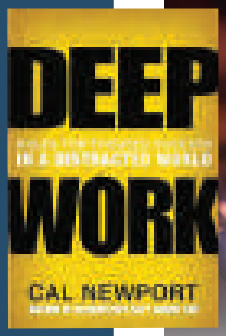
WCI Technology Insider

Insider Tech Tips - Written for Humans, Not Geeks

Deep Work by Cal Newport

In a culture dominated by technology, a rare skill is becoming increasingly more valuable. Deep work is the ability to focus - without distraction - on a mentally demanding task. As people receive a seemingly endless supply of e-mails and engage with an overabundance of social media platforms, they have lost this skill and limited their ability to think critically.



Cal Newport's *Deep Work* does not simply assert that distractions are bad. It focuses on the fact that developing a strong and deep work ethic can greatly produce beneficial outcomes. He also dives into how to transform your mind to think this way.

If you're trying to get ahead of the curve in the workplace, this book is a must-read.

November 2021

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.

A Proven Method to Secure Your Business's Network

People don't usually think about small businesses when discussing cyber security. The media covers breaches in governmental and big-business security in excess. These entities usually have lucrative targets that attract the attention of hackers but are often backed up with an extremely protective network security system that's difficult to crack. When hackers can't break the big system, they turn their attention to easier targets.

While most hackers want the opportunity to crack a high-risk target, these situations are few and far between. Instead, they turn their attention towards much lower-hanging fruit. This is where small businesses come in; they still have access to money and data but have much lower defense that a governmental entity.

Luckily, many average cyber security strategies can keep the would-be hackers away. Their methods are always changing, though, and it helps to be one step ahead of the game.

These are the best current cyber security strategies you can put into place.

Cloud Security

Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage and deletion. As more and more businesses switch from hard-drive data storage to remove databases, this practice is becoming more and more commonplace. Methods of providing cloud

Continued on Page 2 ...

... Continued from Cover

security include firewalls, penetration testing and virtual private networks (VPN), to name a few. While many people feel that their data and information are better stored on a hard drive on their own network, data stored in the cloud may actually be more secure, depending on the system's defense strategy. Be wary, though: not all cloud securities are made the same. Do your research and pick one that will best protect your data.

Network Security

Network security is the protection of the underlying networking infrastructure from unauthorized access, misuse or theft. This is what your network administrator will need to put into place in order to keep your devices and data secure. The best approach to protecting your network is to create a strong WiFi password. Random numbers and letters work best for a small business since nobody but those who need it will be able to guess the password. In addition to a strong password, you'll also have to anticipate any type of internal attack.

"Many average cyber security strategies can keep the would-be hackers away."

VPNs and Firewall

A VPN can help protect your security by masking your IP address. This essentially means that you'll be connected through a different server, making it much harder for the government or websites to pinpoint your location. It also encrypts all network data by creating a secure tunnel A firewall is simply a shield that protects your computer from the Internet. Firewalls can help restrict access to sites that could be damaging to your network. Both of these tools can be highly effective when used properly, but they do not protect against all threats.

Updates and Upgrades

While it might seem simple, consistently updating and upgrading your technology tools can keep you much more secure. The developers of many of these tools are constantly looking for new threats that pose a risk to their program. They'll issue patches to make sure any holes are filled. You just need to make sure that all of your tools are updated in a timely manner and verify that the updates are installing.

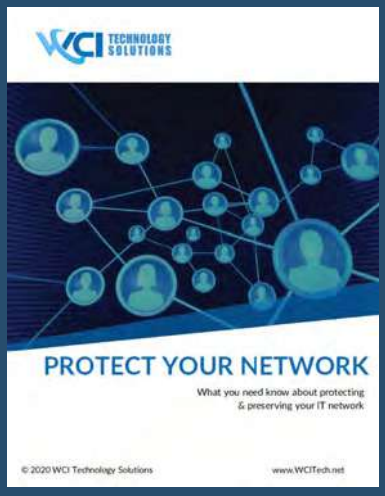
Data Backups

You should always have multiple backups of your business's data. You never know when a power surge of some type of natural disaster might cause your current files to be deleted. You can prevent this issues by regularly backing up your data.

Employee Training

It's important to limit employee access to systems and data owned by your company. Not everyone needs to have access, so only give it to those who can't work without it. There should also be some type of security training for all employees. Phishing schemes and weak passwords create just as many issues as hackers do. Finally, you should make sure everyone in your workplace is security-conscious. A single breach could critically hurt your business. Your employees need to understand this so they can be proactive as well.

No matter which route you take, the most important thing you can for your small business is protect its network.



Free Report Alert: Protect Your Network

This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Get Your Free Copy at www.WCITech.net/protect-your-network

New in Microsoft 365

Pin a chat message in Teams

Now, any member of a chat can pin or unpin a message to the top of a chat header for everyone to see.

People in the chat can click the pinned message. They'll jump straight to the original message in that thread.

Clever, and useful

How much do you think about your browser?

Probably not that much.

We know this, because 75% of Internet Explorer and Edge browsers are out of date.

These are normally updated when your operating system is updated. When you update Windows, Edge get updated. When you update MacOS, Safari gets updated.

If you have an out-of-date browser, this either means that you're not updating your operating system, or you're using a browser that's not native to your operating system (such as Chrome or Firefox).

Either way, please take a moment to check that you don't have any updates waiting to be installed.

Running a browser that hasn't been updated put you at increased risk of security issues. Updates are there to keep you and your data safe. It also means your browset runs faster, and gives you additional features that can help with productivity.

It's simple to check for updates. Just go to www.whatismybrowser.com. It will instantly tell you at the top if you need to apply any updates.

It takes seconds to check if you're running the latest version of your browser. Check it today, and ask your team to do the same. Alternatively, speak to your IT partner, and they can reassure you they're checking and updating on your behalf.

And, if they aren't, give us a call or visit us at wcitech.net today to discuss if there are any improvements to your business's IT needs that we can help facilitate.

Shiny New Gadget of the Month

Angel Guard Cookware

Many people burn themselves every day while cooking in their kitchens. There's a new product on the market that aims to prevent these injuries. After firefighter Eric Le Blanc responded to back-to-back kitchen burns involving children, he knew there had to be a safer alternative. In his research, he found that tipping pots of hot liquid were the world's leading cause of adolescent burns.

Le Blanc developed the world's first tip-proof cookware: Angel Guard Cookware. This cookware removes risk by including a removable stem that slides underneath the burner grate and locks the cookware into place. Now parents no longer have to worry about their child getting hurt after removing a pot from the stove.

Thanking Your Employees

Appreciation is a vital component to keeping your employees happy and productive. More employees feel under-appreciated for the work they do than ever before. Simple gestures such as greeting your employees every day, or buying the team lunch can go a long way toward improving your workplace.

By showing gratitude to your employees, you are acknowledging them as people, and not merely as talents. It also boosts positivity, which helps create stronger leaders and build a better work community. Showing gratitude will improve your relationships with your team, leading to an overall improved work experience. If you're trying to bring everyone together, there truly is no better way than showing gratitude.

Hiring the Best Staff

Not long ago, I had the opportunity to sit down with Carter Cast, the author behind *The Right - And Wrong - Stuff: How Brilliant Careers Are Made and Unmade.* Hiring success has a great influence on career success, and we discussed five negative archetypes that confront employers while filling a job opening. Together, we discovered some telltale signs that your interviewee may fall into one of these categories.

Captain Fantastic

While it might seem like "Captain Fantastic" would be a vital part of your team, they often cause division. Someone who is a "Captain Fantastic" is usually overambitious and has no qualms about stepping on others to get ahead. If you're interviewing a candidate and they mention that their greatest accomplishments revolve around beating others rather than delivering value or developing teams, you probably have a "Captain Fantastic" on your hands.

Solo Flier

Have you ever worked with someone who thinks their way is the best and only way to do something? It's very frustrating. While this type works well individually, they can be detrimental to a team environment. They usually claim to have no time or were too busy to accomplish their tasks; in reality, they may fail to hire and delegate properly. I've met with many people who fit this category and end up leaving their job due to burnout after taking on too much work.

Version 1.0

Change is a necessity in the workplace, but sometimes, people prefer to stick to their routine. To spot these people in interviews, listen to their stories and pay attention if they mention changes in the workplace and how they responded. If they stayed on the same path, that's a red flag. I knew a manufacturing executive who failed to adapt to new technologies. This caused him to lose some of his biggest clients, and the business fell into a tailspin.

The One-Trick Pony

These people usually get stuck in a rut because they rely on their greatest strength to solve *all* problems. They will often aim for lateral moves rather than trying to broaden their horizons. I interviewed a one-trick pony recently who wrote amazing copy, but struggled when meeting with clients face-to-face. His communication skills weren't strong enough to work with clients or lead large teams. his career became stagnant even though he was eager to grow and move up.

Whirling Dervish

Energetic employees improve morale and production in a workplace, but sometimes lack the follow-through need to complete projects. You can usually spot these people in interviews if you notice them avoiding your questions. They often come up with excuses for why they didn't achieve results. Great ideas and strong morale do not make up for a lack of completion.

With knowledge of these archetypes, you can avoid hiring the wrong candidate for your team and instead focus on finding the perfect fit.

Dr. Geoff Smart is chairman & 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 Time* best-seller. He stays active in his community and has advised many government officials.

If you've ever reused a password to sign up for something new, you have a problem

It's something many people admit to doing: they reuse the same password across a few difference services.

Not judging you if you've done it. It's easy to see why thousands of people do this every day. It feels like an easy way to get signed up to something. If you reuse a password, you won't have to go through the hassle of trying to remember it, and needing to reset the password in the future.

However. You only have to do this once, and you're at big risk of something called **credential stuffing.**

This is where hackers get hold of millions of real usernames and passwords. These typically come from the big leaks we hear about in the news.

And then they try all those details to see if they can login to other digital services. They use bots to stuff the credentials into the login box, hence the name.

Because it's automated, they can sit back until their software manages to log into an account... and then they can do damage or steal money.

Stats suggest that 0.1% of breached credentials will result in a successful login to another service.

The best way to protect yourself against theis kind of attack is to never, ever reuse passwords.

Use a password manager to generate long random passwords, remember them for you, and auto fill them. The less hassle for you, the less likely you are to reuse a password. Consider giving a password manager to each of your staff as well.

And if you know you have reused passwords in the past, then you should really change all your passwords on all active services, just to be safe.

If you need a hand, don't forget that a trusted MSP (like us) can guide you.

Did You Know?

about man-in-the-middle attacks?

A man-in-the-middle attack is when a hacker intercepts communication between you and a service you normally use.

For example, they may send you an email pretending to be from your bank. And when you click to login, you're not on the real login page... you're on a fake one that looks real.

By entering your login details, you are handing them to the hacker without even realizing it.

We got our friendly certified ethical hacker to do a man-in-the-middle attack. He filmed both sides so you can see what to look our for. Watch this video now at

www.wcitech.net/hacking

Technology Update

Did you know that sales of PCs are at an all-time high right now? And the types of computers people are buying is changing.

Partly that's been driven by businesses investing in better mobile technology for their teams, to make hybrid working even easier.

An increase in desktop sales is being driven by consumer demand for top end gaming PCs.

I've been reading a market intelligence report (I do this so you don't have to :)), and it says:

Ultra slip laptops now dominate the market with 44.3% of sales

Traditional laptops are the next 26%

Traditional desktops make up 18.1% of sales

One thing that's starting to bite is the worldwide chip shortage. have you heard about this? There's so much demand for chips in all devices, not just computers. Yet supply is down. It's starting to affect many manufacturers, especially those making computers.

So, if you're thinking of upgrading your business's technology, you need to work ahead more than usual.

Question

I've send an email to the wrong person... can I get it back?

ANSWER

Yes, don't panic! In Outlook, open the message in Sent Items, select Actions > Recall this message, the Delete unread copies of this message

Question

Is there an easier way to add appointments to my Outlook calendar?

ANSWER

If you're scheduling a meeting or appointment via email, simply drag that email to your calendar and it will create an appointment for you.

Question

I'm trying to send a photo via email, but it's telling me the file is too large.

ANSWER

The one is easy. Select the photo file you'd like to send. Right click it and select Send To > Mail Recipient. A pop-up window will open which allows you to select the picture size. Click Attach, and it will resize the image and attach it to your message.

Fun Tech Quiz

The person with the lowest score makes the coffee

Can you beat our technology quiz?

1. **Who first came up with the idea of a reprogrammable computer?**
2. **What does the term LASER stand for?**
3. **In what kind of room did computer brands Apple, Dell and Microsoft first get started?**
4. **What does the acronym OS stand for?**
5. **What do you call software that's designed to be modified and improved by others?**

The answers are on page 8.

Tech Fact #1

One Petabyte (PB) = 1,024 Terabytes = 1 million Gigabytes. To put this in perspective, a 50PB drive could hold the entire written works of mankind from the beginning of recorded history ... in all languages

Tech Fact#3

NASA's internet speed in their Washington D.C. HQ is 91GB per second. To put that into context, that's 13,000 times faster than the speed your business currently enjoys.

Tech Fact #2

On average, there is one reply for every 12 million spam emails sent

Tech Fact#4

The American Super Mario Bros. 2 is vastly different from Nintendo's original released in Japan.

Bill's Favorite Business Gadget of the Month

If you switch between your phone and tablet, but also appreciate a full-size keyboard, this is the device for you.

The Logitech K480 Bluetooth multi device keyboard can be connected to several devices at once. It has a little dial to switch between devices. And a cradle built into the keyboard to hold your device at the perfect angle to read while you type.

Inspirational Quote of the Month:

"If you're competitor focused, you have to wait until there is a competitor doing something. Being customer-focused allows you to be more pioneering."

-Jeff Bezos

Answers

1. MATHEMATICIAN CHARLES BABBAGE FIRST CAME UP WITH THE CONCEPT OF A DIGITAL PROGRAMMABLE COMPUTER IN THE 19TH CENTURY
2. LIGHT AMPLIFICATION BY STIMULATED EMISSION OF RADIATION
3. IN THE FOUNDERS' GARAGES
4. OPERATING SYSTEM
5. OPEN SOURCE SOFTWARE

WCI TECHNOLOGY SOLUTIONS

81 Mill Street, Suite 300
Gahanna, OH 43230

@WCITech

WCI Technology Solutions

@WCITech

Is Your Data Secure?

In today's culture, data security is more important than ever. It would be horrific for many if their personal information was compromised. Unfortunately, your data may not be anywhere near as secure as you might hope.

The Pegasus Project is an expose that revealed that a piece of spyware can exploit a user's Apple or Android devices to take control of the user's device. A list of 50,000 victims was published that included government officials, business executives, and even royal family members - proving that no one is safe.

Tech companies usually write extremely secure codes initially, but as new features roll out, holes are created in the defense that hackers can exploit. Pegasus proved that, in the software world, if an adversary is well-motivated, they will find a way in.

The key to staying protected from these breaches is depth. Multiple lines of defense are more protective, so don't stop at one. Though one security tech may have plenty of gaps, another could fill those and strengthen your security.

New security technologies are continuing to advance the security field. There are plenty of actions you can take to ensure that your data remains secure.

Storytelling is More Important Than Building a Presence Online

Social media has become an ever-important tool in the business world. It can help build customer loyalty while also being an essential marketing strategy. However, simply having an account is not enough.

In order to grow, you need to understand your customers and what motivates them. Provide them with an experience they won't be able to obtain anywhere else. Be sure to do this while also making your social media content relevant. If your account does not focus on your products or services, it will prove useless.

Build connections with and focus on your customers. Without trying to approach a specific type of customer, your message can get lost. It can be difficult to attract all of your customers at once.

More important than the rest is to make your presence authentic and accessible. Keep the big picture in mind, and don't get lost in the weeds.