

1st Quarter Newsletter

POCS 2021

COMPUTER SOLUTIONS

Caring for your business as if we own it!

Our physical and mental health is very important. By taking the time to carefully watch what we eat, exercise regularly, and keeping our brain sharp, we can boost our immunity and raise our defenses against exterior threats to our health and well-being.

Although presented in a different form, digital threats can be just as menacing if our cybersecurity skills are not up to snuff. Improving our digital health is paramount to reducing the probability and impact of cyberattacks.

YOUR DIGITAL HEALTH

Just like with our personal health, we all have room for improvements, and failing to stay on top of a regimen can set anyone back to a vulnerable state.

THE LATEST SECURITY
THREATS AND HOW YOU
CAN AVOID THEM



Improving Your Digital Health

As we work to improve our health and well-being on a personal level, it is important to keep your digital health in focus too. Here are some ways to help promote your digital health.



Continue training your brain! Cybersecurity is constantly evolving, so it's important that we keep our brains sharp. As you immerse yourself more in certain topics, you're training your brain to spot the threats.



Boost your immunity! Just like our antibodies can help fend off bad bacteria and viruses in our bodies, we need similar protection on our devices. Ensure all your devices are protected with strong anti-virus protections.



Understand the warning signs! Our bodies send signals such as a fever and fatigue when we are feeling under the weather. Just like with our bodies, our devices may send similar signs such as slow device performance or frequent system crashing.



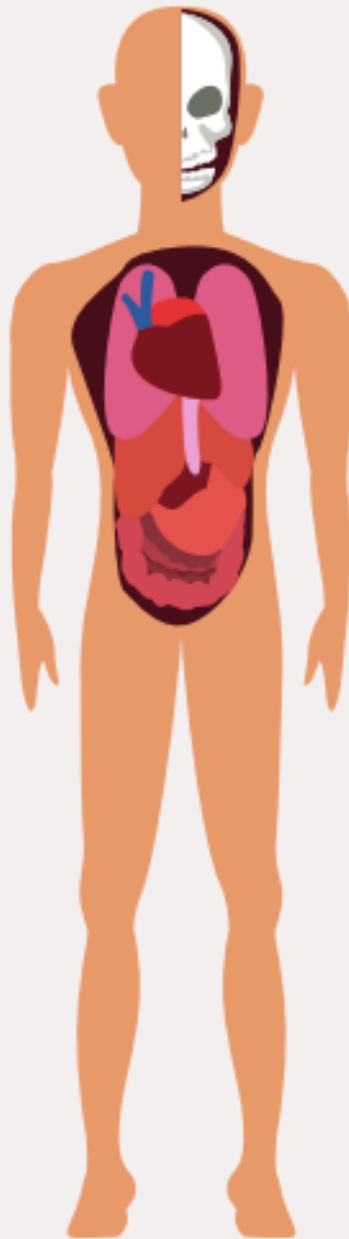
Stay on top of your digital health! To retain control of our physical health, regular appointments with our physicians are important. Keep this process in mind with connected devices too. Create a plan to monitor anti-virus protections and critical updates throughout the year.



Stay healthy! Make sure your devices are getting the appropriate critical updates needed. Just like taking your vitamins, medications, or eating healthy, missing a critical update on a device can leave you vulnerable to external threats.



Flex those muscles! As you train and improve your digital health, don't be afraid to show off your skills. There are many close to you that may not have your knowledge. Share your techniques for cybersecurity excellence with others.





5 Cybersecurity Tips for Small Businesses in 2021

Small Businesses Are A More Common Target For Cyberattacks Than Ever

Many small businesses are sitting ducks for cyberattacks. While large companies may be more likely to face advanced persistent threat (APT) hackers or more complex attacks, many have invested substantial resources in preventing them. Small firms simply lack the security infrastructure of large corporations. They're also more likely to outsource certain functions to third-party vendors, which can also fall victim to cybercrime.

It isn't a surprise that the influx of cyberattacks during the pandemic disproportionately targeted small businesses. Luckily, there are steps small companies can take to protect themselves from breaches.

1. Don't underestimate your company's value to hackers.

Small companies may kid themselves into believing their operation isn't big enough to merit a full-scale security solution. But cyberattacks have not only become more common, they've also grown more sophisticated. Some hackers will steal one company's identity in order to gain access to another company, for example. Small businesses can also stand to lose intellectual property, research, or sensitive customer data.

2. Back up everything.

Ransomware attacks, in which hackers use a type of malware that will prevent companies from accessing their system unless they pay a hefty ransom, have been steadily on the rise. Since 2016, ransomware attacks have risen by 6,000% globally, according to a study by IBM. They've continued to only increase in the wake of the pandemic, with hackers now targeting hospital or health care IT systems.

Companies are still getting locked out of their information because they're not properly backing it up. Make sure you have copies of everything you can't live without.

3. Perform tabletop exercises.

Small businesses should put their cyber readiness to the test. One way firms can do this is by performing a tabletop exercise, or a simulation, of an actual cybercrisis.

Maybe a large chunk of employees neglect to change their passwords every 30 days. Or maybe many of your workers are fooled by a simple phishing scam. Data breaches happen oftentimes because companies are neglecting to follow proper cyber hygiene. Tabletop exercises will help companies realize the weaknesses in their own systems and what they can do to improve.

4. Your cybersecurity budget should reflect your exposure.

Many small companies have limited resources to spend on cybersecurity. When deciding how much to invest in cybersecurity, companies should take into account how much they stand to lose if their data is stolen. A real life example is a small law firm that was the victim of a cyberattack. The firm had one IT employee on staff who had no cyber background. It ended up paying out roughly \$2 million in ransom payments.

If you look at the real loss for them in terms of the intellectual property and the research, etc., it would have been worth the investment to either have an external firm work with them to make sure the data was secure or hire someone within. Understanding what small businesses look like to their attackers is by far the most important thing they should be aware of.

5. Security culture.

Cybersecurity needs to be one of the main goals of your company. It should be part of the working environment. Have the office be one that promotes security culture, so even if a department has nothing to do with IT, they're still making sure to actively participate in keeping the company safe from a cyberattack.



What is an Incident Tabletop Exercise?

An incident response tabletop exercise provides a platform for your security team to discuss, in a classroom-type setting, their roles in response to an incident. A trained expert facilitates the discussion through multiple scenarios to determine the team's readiness or potential gaps. The output of this exercise is to understand your organization's approach to identifying, analyzing, and resolving incidents and how these could be prevented in the future.

The tabletop exercise is often used to validate and/or improve an organization's IR plan. These real-life scenarios put the response plan to the test, highlighting areas where your team excels and areas to be addressed. The tabletop exercise also ensures that everyone on your team knows their roles and responsibilities in the event of an attack. The tabletop exercise aligns everyone's understanding of the due process and empowers the right action through hands-on experience.





RECYCLING

Impacts the World Around Us!

2020 RECYCLING SUMMARY FOR PCS

Item	2020 Pounds	2019 Pounds
Electronics Total	1,821	2,783
Peripherals, PCs, TVs, Laptops, CPUs, Appliances, etc.		

IMPACT OF PCS RECYCLED POUNDS

345
Trees Planted



5,064
Pounds of Gas Reduction



5
Barrels of Oil Saved

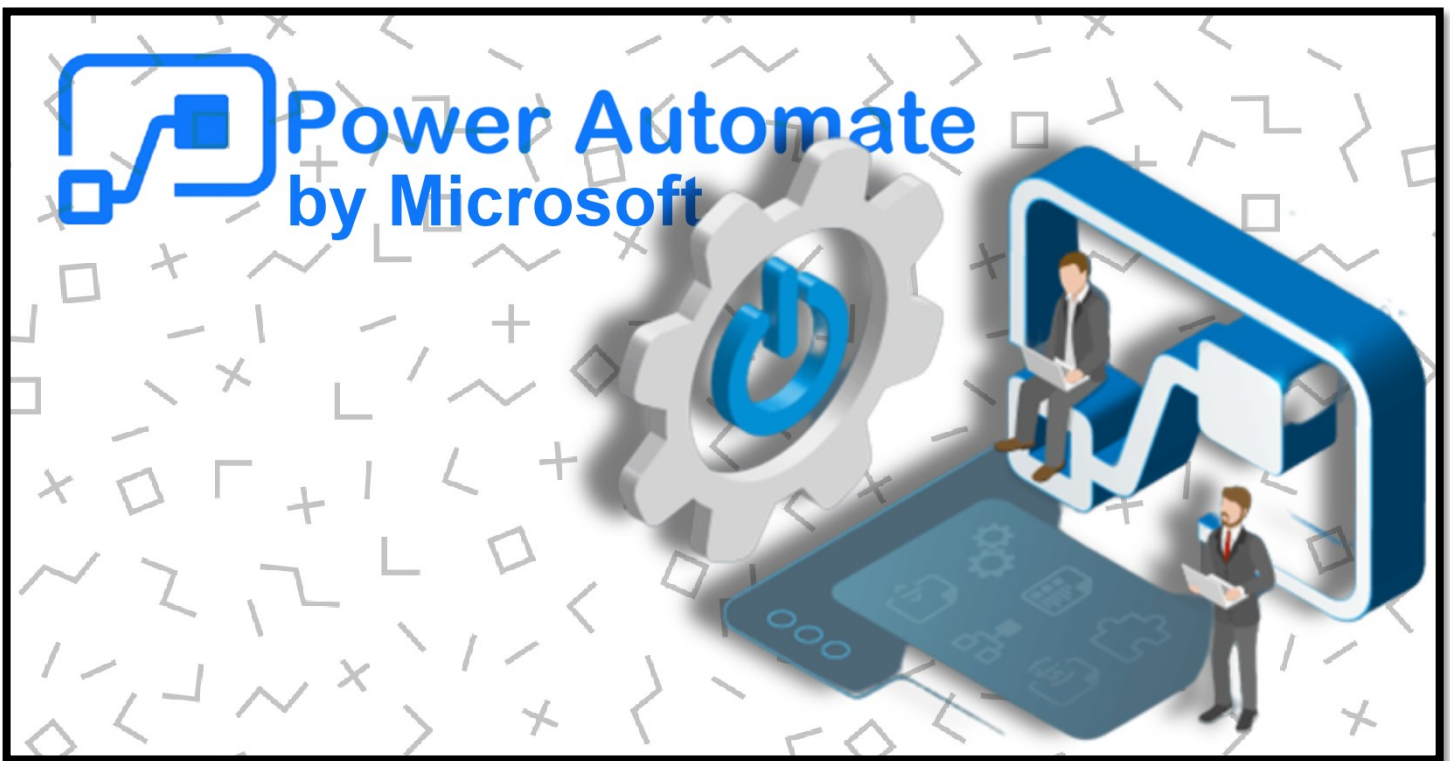


\$570
Environmental Cost Saving



Millions of confidential pages? Thousands of hard drives? Anywhere you store data CyberCrunch has you covered.

CyberCrunch provides data destruction, IT asset disposition (ITAD), and electronics recycling services to businesses, organizations, and government agencies. CyberCrunch specializes in helping businesses to comply with government and industry regulations like HIPAA, PCI-DSS, GLBA and SOX. CyberCrunch provides its services to customers globally from its headquarters in Greensburg, PA and its sister facility in Aston, PA. 866-925-2354



Take care of what's important. Automate the rest.

We live in a world that demands a lot of our attention and keeping up can be a challenge. Did I respond to that last email from my manager? Did I send the updated contract? How do I stay on top of approvals?

There's an easier way to manage your daily business processes. Microsoft Power Automate is an intelligent, cloud-based solution that uses triggers and actions to create chain reactions within your normal workflow. So that repetitive, manual, time-consuming tasks get done without you lifting a finger, or writing a single line of code.

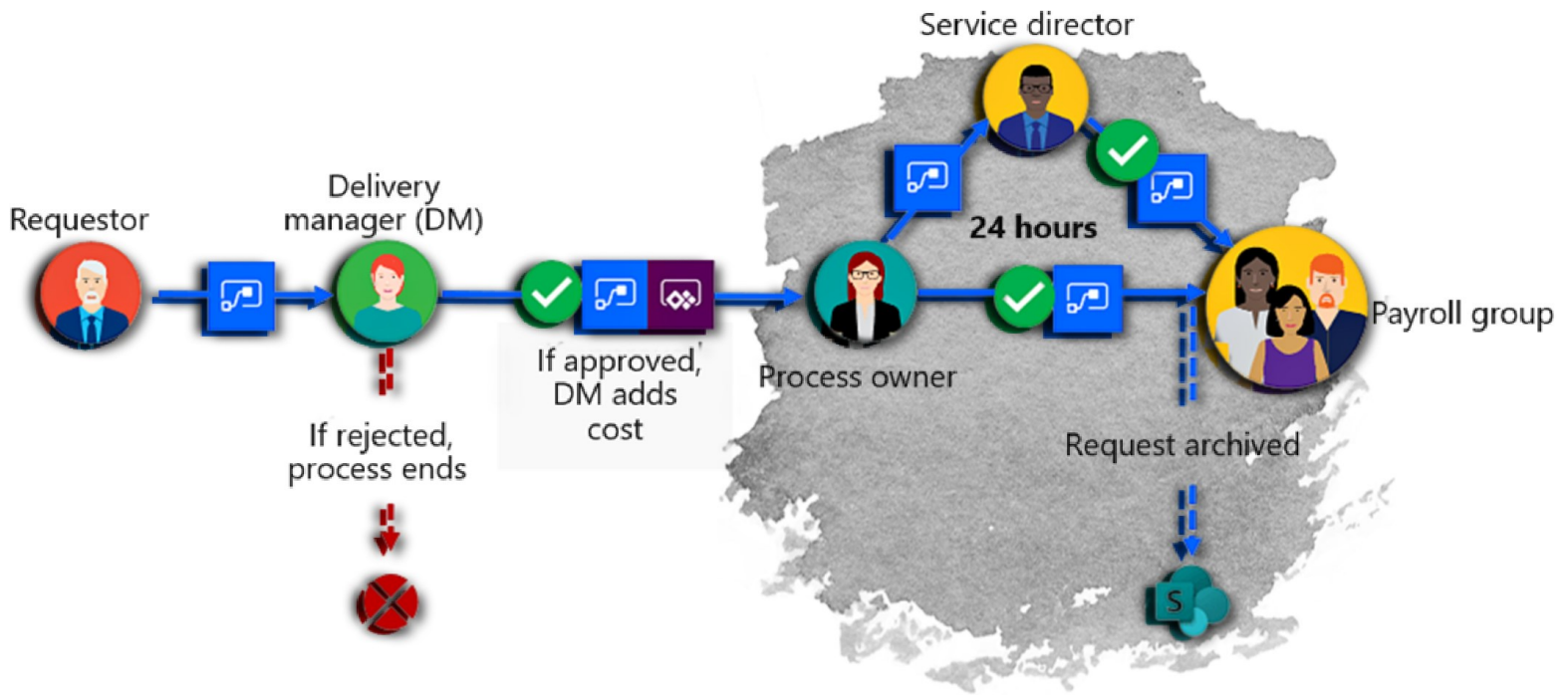
All you have to do is set the trigger and then, Power Automate takes care of the actions that come next. All of these triggers and actions come together in one integrated ecosystem that offers thousands of pre-built templates and hundreds of connectors so you can customize your automations and fully automate your work.

Turn outdated into automated

Streamline repetitive tasks and paperless processes with Microsoft Power Automate—so you can focus your attention where it's needed most.

Boost productivity

Build time-saving workflows into everything from individual tasks to large-scale systems with seamless integration using hundreds of prebuilt connectors.



Automate quickly and more securely

Enable everyone to build secure workflows with a low-code, no-code guided experience to automate mundane everyday tasks with robotic process automation (RPA).

Put intelligent workflows to work

Automate time-consuming manual tasks with built-in AI capabilities, giving you more time to focus on strategic, high-value opportunities.

What can you expect from Power Automate? Here are a few examples of what you can do:

- Automate business processes
- Send automatic reminders for past due tasks
- Move business data between systems on a schedule
- Connect to almost 300 data sources or any publicly available API
- You can even automate tasks on your local computer like computing data in Excel.

And because Power Automate is from Microsoft, it's built for getting things done. Microsoft Power Automate democratizes intelligent automation by empowering everyone, whether they're an end user, on the front line of business, or an expert at the forefront of technology, to seamlessly build secure, automated workflows so they can scale automation and focus on strategic work that drives their business forward. Microsoft Power Automate. Automation for all.

Ready to learn more?

Give the experts at PCS a call. 724-942-1337



WHAT'S THE DEAL WITH COOKIES?

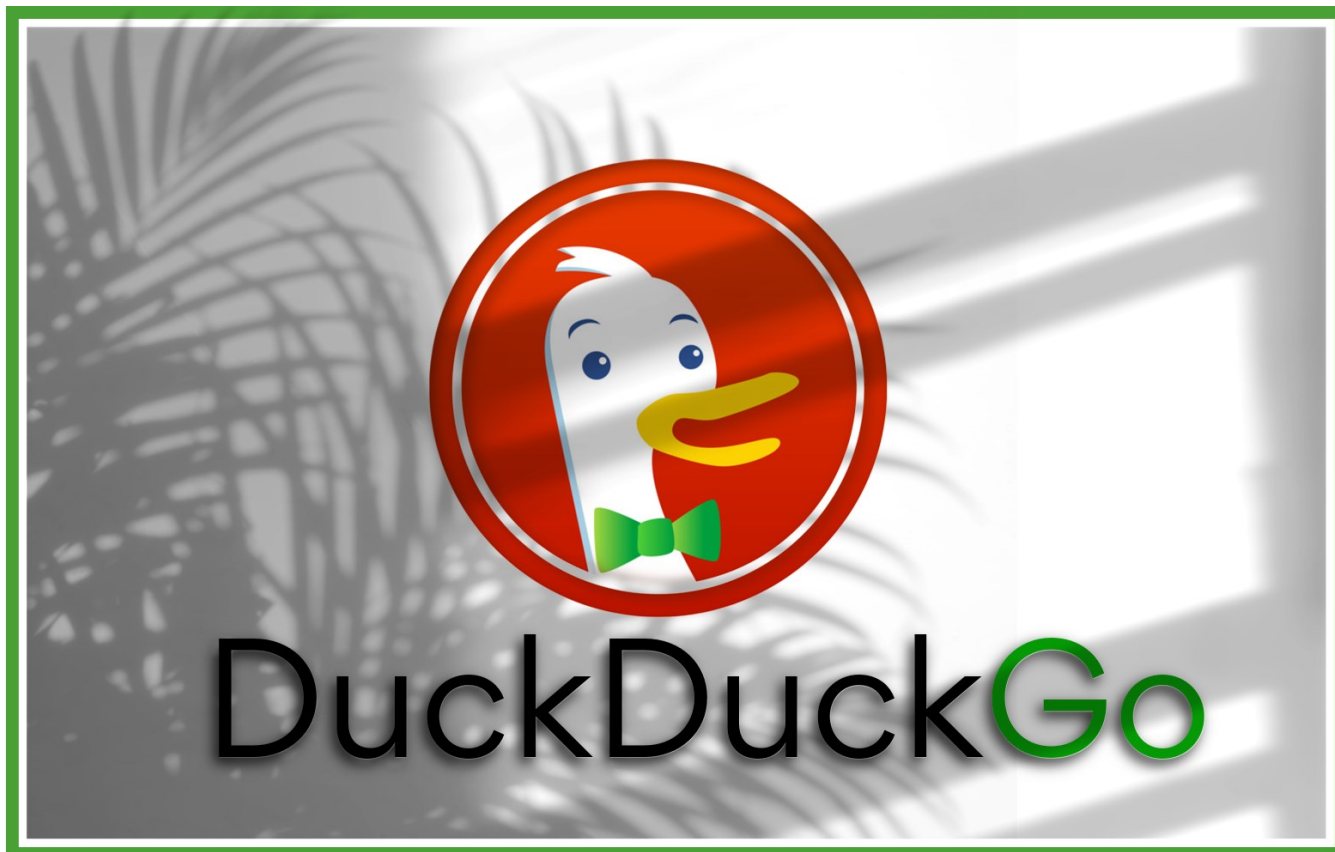
An internet cookie is a website's way of keeping track of its visitors and their activity. As they collect data, cookies can help the website optimize the user's experience with login assistance, advertisement management and preference settings.

Cookies by themselves generally don't pose a large security risk to most users, however malicious cookies could be delivered by malicious webpages. The best advice is to browse carefully, avoid suspicious websites, and keep your browser up to date to avoid security flaws.

The bigger issues with cookies lay with the privacy concerns. Nearly every website you visit will try to use a cookie in some way, but again these are not meant to be negative for the user but rather for their convenience.

Many websites will present their visitors with a banner or pop-up regarding their use of cookies, and how the user can accept the cookies, or some sites will allow you to manage certain cookies. Managing cookies from your browser may be easier to take more control over halting the data collection. Within your internet browser, you should have the ability to control many settings such as blocking cookies, setting up sites that can or cannot use cookies, clearing cookies after closing the browser, and more.

Each internet browser is different in what is available and how it is accessed but try going into your Settings and looking for Privacy and Security settings. You can also consider using a private browsing session that your internet browser may come equipped with. This private browsing session will restrict many cookie operations as you surf the web.



Meet the Google Alternative for Privacy

Ever notice ads constantly following you around? That's in part because Google tracks your searches and hides trackers on millions of websites. By contrast, DuckDuckGo is an internet search engine that emphasizes protecting searchers' privacy and avoiding the manipulation of the filter bubble of personalized search results.

DuckDuckGo distinguishes itself from other search engines by not profiling its users and by showing all users the same search results for a given search term.

You can also make DuckDuckGo your default search engine in browsers like Chrome, Safari, Firefox, and Edge. Whenever you search from your browser's location bar or new tab page, you'll be taken to DuckDuckGo instead of Google. DuckDuckGo is built into modern web browsers as one of the default options, and switching just takes a few clicks or taps.

DuckDuckGo looks a lot like Google. It can search websites, images, videos, news articles, and shopping web pages. It has built-in maps with navigation powered by Apple Maps. It has dictionary results, Wikipedia integration, and other instant answers, just like Google does.

DuckDuckGo is owned by a company named Duck Duck Go, Inc. The company is based out of Paoli, Pennsylvania, and it has 124 employees around the world as of January 2021. This search engine was launched in 2008, more than a decade ago. Since then, DuckDuckGo's traffic continues to climb to new heights. As of January 19, 2021, more than 102 million searches are being performed on DuckDuckGo each day.
