the Tech Chronicle

The Official Newsletter of NorthStar Technology Services

212 W. Route 38, Suite 103
Moorestown, NJ 08057

Trusted. Reliable. Secure.

The Official Company Newsletter of NorthStar Technology Services

IN MARCH'S ISSUE

- Cyber Attacks
- Client Spotlight
- February Tech Tip Recap
- Working From Home
- Tech Trivia Time
- Microsoft Forms
- 3 Step Work-Life Balance

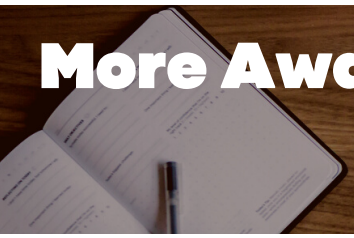
Let's Connect:

northstartechs
northstartechs
NorthStar Technology Services
NorthStar Technology Services
www.northstarsvc.com
(856) 375-1220
info@northstarsvc.com

MAR. 2023 | VOL. 6

the Tech Chronicle

The Official Company Newsletter of NorthStar Technology Services



More Aware? More Prepared

We're Sharing About Today's Most Common Types Of Cyber-Attacks

If you've watched the news lately, you've probably heard about businesses getting shut down due to cyber-attacks. Don't think you're immune just because you're a small business - hackers can come after anyone. It's important to be ready to defend your business from cyber threats because they can nab your private info, your customers' data, and your employees' info too. The damage to your reputation and bank account could be huge.

If you're a business owner or leader looking to keep your company safe from cyber threats, it's important to stay informed about the most common types of cyber-attacks that companies are facing today. By learning about these threats, you can take action and implement effective cybersecurity plans and tactics to keep your business protected from cybercriminals.

Phishing Attacks

Phishing is a fraudulent tactic where cybercriminals send deceptive messages to trick people into revealing sensitive information or downloading malicious software. These scams can have devastating effects on both personal and business life. For instance, you may have received an email from someone pretending to be Amazon or your credit card company, asking for private information. However, the sender's email address may not match their supposed identity.

When your business falls victim to a phishing scam, cybercriminals may request valuable information from your employees, such as passwords or customer data. If your staff members fall for the scam, the cybercriminals can gain unauthorized access to your systems and steal sensitive employee and customer information, leaving your workforce exposed to identity theft. To prevent these scams, it's important to exercise common sense and provide cybersecurity training to your employees. Most legitimate companies will not request confidential information via email. However, if an employee receives a suspicious email, they should take the time to verify its authenticity before responding or sharing any confidential information.

Malware

Malware is software that can be installed on a computer without the user's permission and can cause harm by stealing sensitive information, such as passwords or money. Various types of malware exist, including viruses, spyware, ransomware, and adware. Accidentally downloading malware can happen when clicking on dubious links in emails or websites, and you may not even realize that your computer has malware on it. Signs of malware include slow computer performance, random web browser redirects, and frequent pop-ups. If you notice any of these, it's essential to scan your computer for malware.

Preventing malware from infecting your business is critical. Employing a managed services provider who continuously monitors your network for security gaps is the most effective way to protect your business. When it comes to malware, it's better to be safe than sorry. If a cybercriminal deploys ransomware on your network, your business may come to a halt until the ransom is paid. Even if you pay the ransom, your reputation may still suffer, and your business and your clients could be significantly impacted.

Continued on pg. 2

CLIENT SPOTLIGHT

JSA

JAMES SASSANO ASSOCIATES ENGINEERING

JSA Engineering has been a trusted partner with home builders, developers, contractors, architects, and municipalities since 1996. JSA offers a comprehensive approach to all engineering, surveying, planning, and construction layout needs by staying current with the land use laws and regulations. They additionally have a team of licensed professional designers and technicians utilizing the most current design software and office technology, including GPS and robotic surveying. Their clients range from individual landowners to large contractors, developers, and national builders throughout New Jersey, Pennsylvania and they welcome projects of any size! NorthStar has supported JSA's tech and security systems since 2014, creating a long-lasting business relationship. We look forward to many more successful years for both our organizations!

This monthly publication is provided courtesy of **Eric Williams**, the CEO, Owner, & Founder of NorthStar Technology Services located in Moorestown, NJ.

NORTHSTAR TECHNOLOGY SERVICES, LLC

Our Mission:

To build a community of successful-minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

We are proud to have served the greater Philadelphia Metro Area since 2008.

Continued from pg. 1

Don't completely relax when you're using your phone either, as malware attacks on mobile devices have become more prevalent in recent years.

Password Attacks

How do your employees log into your systems? Chances are, they use a password to access their computer, email, and more. But what if a bad guy got a hold of one of those passwords? They could potentially (and likely would) steal sensitive info about your company, customers, and employees.

Make sure your team is using long, complex passwords for each account, and never reuse the same password twice. Encourage them to use password managers to create the strongest passwords possible and keep track of them easily. Additionally, consider using two-factor authentication to create another layer of security. Be sure to include all of this in your annual security training.

Getting hit by a cyber attack can compromise your business and cause widespread damage, so **now** is the time to take protective action. Knowing the most common types of attacks is a good start. You're aware and (hopefully) more prepared – now get to work on those protection plans!

Tech Tip Recap

Remove Unused Apps From Your Phone

Delete apps that are taking up unnecessary space to free up space on your phone and help it run smoother.

Reopen Tabs You Just Closed

PC users hold down the Ctrl, Shift, and T keys, and Mac users hold down the Command, Shift, and T keys!

Increase Computer Speed

Uninstall unused software, limit the software that opens when you turn on your computer, add more RAM (random access memory), and always check for malware!

Create A Strong Password

Use a password manager, keep the password length long, and use some variety when creating your passwords for ultimate protection.

Follow Our Socials For Weekly Tech Tips!

Maybe you shouldn't go back to work.

Don't come back to work. Instead, move forward in leading your company and managing your career by embracing remote work. Even though ghSMART has been remote-only for over 26 years, I never fully realized how enthusiastic I am about remote work until I heard that many companies are forcing workers to come back into offices.

Before the COVID-19 pandemic, "work where you want" was a rare concept – but during the pandemic, basically every company that could function with people working remotely shifted to that mode out of necessity. I thought that mode would stick, and we'd see the landscape of cities shift from "places people go to work every day" to "places people go to work sometimes, eat, shop, learn and play." But it seems I was wrong.

There isn't a great argument against the idea of remote work, but there is one for it. Remote work improves financial and operating performance and productivity for companies while also improving job and life satisfaction for employees. A 2015 Stanford University study published in the Quarterly Journal of Economics showed a 13% performance increase from remote working, and employee attrition rates fell by 50%.

Even with all of the research and information available that shows remote work is beneficial, there are still some myths floating around. For example, many say you can't build a great company culture when your business operates remotely. This is false.

I think an excellent culture begins with doing what's best for people. Making people commute to offices daily does not seem to be in anybody's best interests.

Another common myth states that people don't work as hard remotely as they do in an office. I believe if you have a transparent culture where performance is measured, you can pay people according to the value they are creating. They will be incentivized to work productively and not lollygag – even if they are working remotely. Many companies have not yet figured out how to pay employees based on a scorecard of measurable results and instead pay based on hours worked. They should be worried about lollygagging anyway, both in the office and for people who work remotely.

If you run or own a company, please continue to experiment with allowing your people to work remotely when possible. I believe this is the future of work, both because of the demonstrable benefits to companies in operating and financial performance and the benefits to workers due to having more control over their time.

Dr. Geoff Smart is the chairman and 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 Times bestsellers. He stays active in his community and has advised many government officials.

Comic Corner

"Frankly, we're stumped. So, we'd like to try turning you off and then on again"

Everyone is missing out.

Microsoft 365 is a popular software used widely across the globe, with approximately 345 million subscribers. It offers more than 20 applications, including the renowned MS Office suite. However, due to the abundance of options, some apps end up overlooked.

Many companies are not even aware of some of the other useful applications available to them. One of these useful applications is Microsoft Forms.

So, what's Microsoft Forms?

Microsoft Forms is a tool that lets you create forms, quizzes, and surveys with ease. You can easily share your survey by link and let users fill it out from any device.

How to Get Started in Forms:

1. Visit Forms.office.com and log into your Microsoft account.

2. Choose “New Form” or “New Quiz" from the top menu.

3. OR you can choose to explore the built-in templates.

4. Click “Add New” to add a new form field. You can choose from field types such as:

- Choice (i.e., multiple-choice question)
- Text
- Rating
- Date
- Ranking
- Likert (a scale that records attitudes/opinions about a topic)
- Net Promoter Score® (a scale from “not likely” to “extremely likely”)
- Section (separator that can include a title and image)

5. Enter your questions

6. Once you're finished, click “Send” at the top. You can distribute the survey using the following options:

- Link to a web form
- Email
- QR code
- Embed in a web page
- Via Facebook or Twitter

7. View responses on the “Responses” tab

Advantages of Using Microsoft Forms

It’s Included in Microsoft 365 Subscriptions

If you already subscribe to Microsoft 365, you automatically get access to MS Forms.

It Saves Time

No emailing attachments back and forth, and Forms collates survey responses automatically.

Get Charted Results

You can quickly see the results of the survey in meaningful graphs.

It’s Easy to Use

There’s a very low learning curve with Microsoft Forms.The interface is intuitive and simple, so just about everyone can jump in and start using it.

How You Can Leverage MS Forms:

- Annual Customer Satisfaction Survey
- Employee Security Awareness Quiz
- Change Readiness Survey
- Event Registrations
- Volunteer Registration Form

ITS TIME FOR...

Tech Trivia

It's time for Tech Trivia where we ask our readers a question! The answer is posted under the month's newsletter PDF on our website newsletter page, found under the "Resources" tab.

The question this month is:
Where did the word “Bluetooth” originally come from?

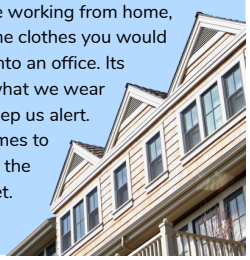
Improve Work-Life Balance

As more companies switch to remote work, some employees struggle to find that work-life balance. They end up constantly drawn back to work, leaving hardly any time for their hobbies or family. It's important to maintain that healthy work-life balance for our well-being and productivity. Here are three tips to stay productive during work hours and help create that time for yourself:

Set Boundaries: Don’t allow yourself to be pulled back into work. Turn off your work phone and e-mail when your shift has ended for the day.

Create A Workspace: Do not work in the same areas you use for relaxation. This will make it difficult to focus when you work and difficult to relax when you’ve finished working.

Dress Professionally: It might be tempting to wear sweatpants while working from home, but try to wear the same clothes you would wear if you had to go into an office. Its incredible how much what we wear can motivate us and keep us alert. When the workday comes to a close, you can switch the clothes **and** the mindset.



Follow Us!

northstartechs
northstartechs
NorthStar Technology Services
NorthStar Technology Services

SCAN ME

Did you know we offer a cyber security assessment?

This *no-risk* and *high-return* assessment will tell you whether your company is fully secure. Even if you already have in-house IT or a tech MSP, a routine check up is not only recommended but vital to your company's success.

Scan the QR code or visit this link to learn more: https://www.northstarsvc.com/discoverycall/