MONTHLY NEWSLETTER

SEPTEMBER 2024

TECH "KNOWLEDGY"

Ransomware

A newsletter article by Berry Solutions Group

In today's digital age, cyber threats are evolving at an unprecedented pace, and one of the most pervasive and damaging threats is Ransomware. Imagine waking up to find that all your important files and data are locked, with a message demanding payment to regain access. This is the harsh reality of a Ransomware attack.

Ransomware is not just a buzzword; it is a serious cybercrime that can cripple businesses, disrupt services, and lead to significant financial losses. From small businesses to large corporations, no one is immune. The impact of Ransomware extends beyond financial damage, affecting reputations and operational capabilities. One in particular known as RansomHub has encrypted and exfiltrated data from at least 210 companies since February of 2024 representing the water and wastewater, information technology, government services and facilities, healthcare and public health, emergency services, food and agriculture sectors to name a few.

What is Ransomware?

Ransomware is a type of malicious software that encrypts your files, making them inaccessible. Attackers then demand a ransom to restore access. This can lead to significant disruptions, data loss, and financial costs.

Why is Awareness Important?

Understanding Ransomware and how to protect against it is crucial. Ransomware attacks can impact anyone, from large organizations to individual users. By being informed, you can take proactive steps to safeguard your data and systems.

How to Protect Yourself:

1. Keep Software Updated: Regularly update your operating systems and applications to patch vulnerabilities.
2. Use Multi-Factor Authentication (MFA): Add an extra layer of security to your accounts.
3. Employee Training: Highlight the need for ongoing employee training programs that cover the latest ransomware tactics and prevention strategies. This can include simulated phishing attacks to test and improve employee awareness.
4. Regular Security Audits: Emphasize the importance of conducting regular security audits and penetration tests to identify and address vulnerabilities before they can be exploited by attackers.
5. Incident Response Plan: Include a section on creating and maintaining an incident response plan. This plan should outline the steps to take immediately after a ransomware attack, including isolating affected systems, notifying relevant stakeholders, and contacting law enforcement.

Resources for Further Information:

For more detailed information on ransomware and how to protect yourself, please visit the CISA #StopRansomware Guide.

By following these best practices, organizations can significantly reduce the risk of Ransomware attacks and enhance their overall cybersecurity posture. If you need more detailed information on any of these strategies, feel free to ask us!

SECURITY CORNER

Phishing: The Path to Ransomware

One of the most popular phishing scams impacting businesses today is a sophisticated con where cybercriminals exploit calendar invites to trick individuals into clicking malicious links. These invites often appear legitimate, coming from seemingly trusted sources, and include urgent or enticing messages to prompt immediate action. To spot calendar phishing, look for unusual or unexpected invites, especially those with generic or urgent language. Always verify the sender's email address and be cautious of any links or attachments within the invite. If something seems off, contact the sender through a different communication channel to confirm the legitimacy of the invite.

To avoid falling victim to calendar phishing, it's crucial to adopt good cybersecurity practices. Disable automatic calendar invite additions to prevent unsolicited invites from appearing in your calendar. Use multi-factor authentication (MFA) to add an extra layer of security to your accounts. Regularly update your software and educate yourself and your employees about the latest phishing tactics. By staying vigilant and informed, you can protect your personal and business data from these sophisticated attacks.

EMPLOYEE CELEBRATIONS & SPOTLIGHT

BSG is pleased to announce that Garrett Houghton will be transitioning into a new role within our organization as Manager of Systems. In his new position, Garrett will be responsible for managing our Internal Business applications and server environment as our system administrator in addition to developing training materials and course content within BSG while also helping us implement internal quality assurance policies and procedures.

Garrett has been professional in the IT industry for 9 years, beginning as a substitute instructor at the Commonwealth Technical Institute, where he also earned his Associate Degree in Network Technology, with a certification in Fiber Optic Cabling. After his teaching stint, Garrett transitioned to a role as NOC Lead at a Managed Service Provider, honing his skills in network operations and management.

In 2020, Garrett joined Berry Solutions Group, where his dedication and contribution as the Service Desk Manager was quickly recognized. During this time, he also obtained his ITIL certification and assisted in developing many internal processes, procedures, and accompanying documentation.

Outside of his professional life, Garrett is an avid fan of the Harry Potter series and enjoys participating in a bowling league. His passion for technology and continuous learning, combined with his hobbies, make him a well-rounded individual both in and out of the workplace.

Please join us in congratulating Garrett on his new position!!

Employee Anniversaries:

September 11 – Ryan Farabaugh (1 yr)
September 21 – Garrett Houghton (5 yr)

BSG welcomes the following new employees:

Aaron Trusky
Director of Systems

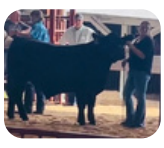
Trevor Musser
Team Service Desk

Philip Bastian
Account Manager

BSG IN THE COMMUNITY

Thanks to Berry Family Farms for hosting our annual summer picnic!

Employees and their families had the opportunity to relax and enjoy some great food, along with a lively cornhole tournament!



4-H Sale

BSG is proud to support the local 4-H sale, hosted annualy by the Penn State 4H Extension Office, at the Bedford County Fair. We offer our congratulations to all participants and are happy to share in the effort to promote life-long learning opportunities!

TECH TIPS & TRICKS

★ ***Employee Favorites!*** ★

- **Pin Favorite Apps to Taskbar:** Right-click on frequently used apps and select Pin to taskbar for quick access.
- **Use File Explorer:** Open File Explorer with Windows + E to quickly access your files and folders.
- **Take Screenshots Easily:** Press Windows + Shift + S to snip a portion of your screen and save it to your clipboard.
- **Customize the Start Menu:** Right-click on app tiles in the Start menu to resize or remove them for a cleaner look.
- **Use Windows Search:** Press Windows + S and type what you're looking for to quickly find files, apps, or settings.
- **Dark Mode:** Reduce eye strain by enabling Dark Mode. Go to Settings > Personalization > Colors and select Dark under "Choose your color"
- **Snip & Sketch:** Take screenshots and annotate them using the Snip & Sketch tool. Press Win + Shift + S to start a new snip
- **Clipboard History:** Enable clipboard history to access multiple copied items. Press Win + V to view your clipboard history
- **Win + Ctrl + Shift + B:** Reset your display driver, useful if your screen freezes
- **Win + Plus (+):** Open Magnifier and zoom in
  • Win + Minus (-): Zoom out with Magnifier

UPCOMING EVENTS

September 9, 2024: Small Business Empowerment Summit

This summit is a forum for collaboration, discussion, and interaction between the Commonwealth of Pennsylvania, federal agencies, elected officials, vendors, and the small business community. Small businesses who attend the Empowerment Summit will gain a better understanding of Commonwealth and federal procurement opportunities, as well as resources to access capital to launch, grow, and increase their business capacity.

October 2-3, 2024: CyberSecurity Summit 2024

Join over 600 thought leaders and security experts from the state government and local government, federal agencies, K-12 school districts, higher education, as well as technology leaders in the private sector for this year's event. BSG will be co-presenting a topic with Reclamere at this event on AI for Hacking and Security