MONTHLY NEWSLETTER

DECEMBER 2024

TECH "KNOWLEDGY"

The Hidden Dangers of IoT Devices: Securing Your Smart Home and Business from Cyber Threats

A newsletter article by Berry Solutions Group

The proliferation of Internet of Things (IoT) devices, including seemingly innocuous items like LED Christmas lights, presents significant security challenges. These devices often lack robust security features, making them vulnerable to hacking and unauthorized access. Many IoT devices are designed with convenience in mind, prioritizing ease of use over security. This can lead to weak default passwords, unencrypted data transmission, and infrequent software updates, creating multiple entry points for cybercriminals. Once compromised, these devices can be used to infiltrate home networks, access sensitive information, or even launch larger-scale attacks such as Distributed Denial of Service (DDoS) attacks.

The sheer number of IoT devices connected to the internet exponentially increases the attack surface for potential cyber threats. Each connected device represents a potential vulnerability. For instance, if an LED Christmas light system is hacked, it could serve as a gateway to other connected devices within the same network, such as smart thermostats, security cameras, or personal computers. This interconnectedness means that a breach in one device can compromise the entire network, leading to significant privacy and security risks.

Moreover, IoT devices often collect extensive and sensitive data, ranging from personal preferences and habits to location data and video footage. If this data is not adequately protected, it can be intercepted and misused by malicious actors. The lack of standardized security protocols across different IoT devices exacerbates this problem, creating inconsistencies in how data is protected and managed. As the adoption of IoT devices continues to grow, it is crucial for manufacturers to implement stronger security measures and for consumers to be aware of the potential risks and take steps to secure their devices.

Introducing a new wireless gadget into your home can compromise your security because attackers no longer need physical access to breach your devices. They can use methods like impersonation, brute-forcing, or Man-in-the-Middle (MITM) attacks. While some manufacturers follow best cybersecurity practices, many do not, especially with cheaper smart devices. This disparity insecurity standards means that even a simple smart light bulb can become a vulnerability.

When you secure your home, you use a key to prevent unauthorized entry, and your internet router provides a secure network. However, by installing an innocent-looking smart bulb outside, you might be opening the door to potential hackers. Attackers can connect to the smart bulb, retrieve its settings and code, and extract your Wi-Fi credentials, gaining access to all devices within your home. This scenario highlights the importance of considering security risks before adding new IoT devices to your network.

SECURITY CORNER

Ransomware Awareness for Holidays and Weekends

The Cybersecurity and Infrastructure Security Agency (CISA) and the FBI have noted a rise in ransomware attacks targeting U.S. entities during holidays and weekends when offices are typically closed. These attacks take advantage of the reduced IT and security staff during these times, allowing cybercriminals to deploy ransomware and spread it across networks more effectively. Notable incidents include the DarkSide ransomware attack on a critical infrastructure entity in the Energy Sector during Mother's Day weekend and the Sodinokibi/REvil ransomware attacks on the Food and Agricultural Sector over Memorial Day and the IT Sector during the Fourth of July holiday.

Ransomware attacks have evolved beyond simple data encryption to include data exfiltration and threats to publicly release sensitive information, increasing the pressure on victims to pay ransoms. The FBI's Internet Crime Complaint Center (IC3) reported a significant rise in ransomware incidents and ransom demands in 2020 and 2021. Common initial access methods for these attacks include phishing, brute-forcing unsecured remote desktop protocol (RDP) endpoints, and exploiting software vulnerabilities. Cybercriminals also use precursor malware to conduct reconnaissance, steal credentials, and move laterally within networks before deploying ransomware.

To mitigate these threats, CISA and the FBI recommend several proactive measures, including making offline backups of data, securing and monitoring RDP, updating operating systems and software, using strong passwords, and implementing multi-factor authentication. Organizations are also encouraged to engage in threat hunting to detect and respond to potential threats before they can cause significant damage. By understanding normal network activity and establishing baselines, organizations can better identify and respond to anomalies that may indicate aransomware attack.

EMPLOYEE CELEBRATIONS & SPOTLIGHT

Cody Virgillo followed his interest in Computer Networking beginning in high school, when he spent his Junior and Senior years attending the Computer Systems Networking class at Admiral Peary Area Professional Technical School. Following completion of the 2-year course, Cody received a Pennsylvania Skills Certificate. He continued his studies at South Hills School of Business &Technology, obtaining an associate degree in Specialized Technology in Information Technology.

His employment with Berry Solutions Group began in February 2021. Since that time, Cody has obtained his CompTIA A+ certification. He enjoys working on the Veeam backup solution, and assists with tickets and projects, while also providing on-site support to clients.

In his spare time, Cody enjoys mountain biking, riding motorcyles, playing video games, going to car shows, watching and adding supercross races, and watching movies and TV shows. He is a self-proclaimed Star Wars and Harry Potter nerd!.

December 11, 2024 marked Cynthia Welsh's one-year anniversary with Berry Solutions Group. Thanks for everything you do, Cynthia!

BSG IN THE COMMUNITY

On November 3rd, BSG participated in the 3rd annual Strike Out Child Abuse bowling tournament in support of Circle of Support Child Advocacy Center.
2 Teams were represented at the tournament: Berry Bad Bowlers and Bowling Stones! The event supports the CAC mission of providing services to child abuse victims and their families. Since the opening in 2015, the CAC has provided services to over 2100 children. BSG is proud to support the organization in their mission!

TECH TIPS & TRICKS

Tech Tips and Tricks

- Use Focused Inbox: This feature helps you manage your emails by sorting them into two tabs: Focused and Other. Important emails go to the Focused tab, while less important ones go to Other. This way, you can prioritize your attention on what matters most.
- Schedule Emails: If you want to send an email at a specific time, you can schedule it. Compose your email, then go to the Options tab and select "Delay Delivery." Set the date and time you want the email to be sent, and Outlook will handle the rest.
- Quick Steps: Automate repetitive tasks with Quick Steps. For example, you can create a Quick Step to move emails from a specific sender to a designated folder with one click. This can save you a lot of time and keep your inbox organized.
- Use @Mentions: To get someone's attention in an email, use the @ symbol followed by their name. This highlights their name in the message and adds them to the To line, ensuring they see the email.
- Keyboard Shortcuts: Familiarize yourself with Outlook's keyboard shortcuts to navigate and perform tasks more efficiently. For instance, use Ctrl + R to reply to an email, Ctrl + Shift+ M to create a new email, and Ctrl + 2 to open your calendar.
- Create Search Folders: If you frequently search for the same types of emails, create a Search Folder. This folder automatically updates with emails that match your search criteria, making it easier to find what you need.
- Use Rules to Manage Your Inbox: Set up rules to automatically sort incoming emails. For example, you can create a rule to move all emails from a specific sender to a designated folder, helping you stay organized and reducing inbox clutter.
- Turn Off Notifications: Reduce distractions by turning off email notifications. You can customize which notifications you receive, so you're only alerted to the most important emails.
- Use the Scheduling Assistant: When setting up meetings, use the Scheduling Assistant to find a time that works for everyone. This tool shows you the availability of your invitees, making it easier to schedule meetings.
- Customize Your Swipe Options: On mobile, you can customize swipe actions to quickly manage your emails. Go to Settings, then Swipe Options, and choose actions like delete, archive, or mark as read.