BERRY SOLUTIONS GROUP

MONTHLY NEWSLETTER

OCTOBER 2024

TECH "KNOWLEDGY"

AI for Hacking and Security: Navigating the Dual-Edged Sword

A newsletter article by Berry Solutions Group

Understanding the Threat Landscape

Artificial Intelligence (AI) is revolutionizing the cybersecurity landscape, but not always for the better. Hackers are increasingly leveraging AI to develop sophisticated methods of attack. These include machine learning algorithms to identify system vulnerabilities, AI-powered phishing to craft highly convincing fake emails, and deep learning malware designed to evade traditional security measures. These advancements pose significant threats to companies, making it crucial to understand and anticipate these AI-driven hacking techniques.

Harnessing AI for Defense

Fortunately, AI is also being utilized to bolster security defenses. AI-powered security tools are employed in various domains, including endpoint protection, network defense, and cloud security. These tools use machine learning and behavioral analysis to detect and prevent attacks by analyzing patterns and anomalies in data. Integrating these AI-based security measures enhances the overall security posture of organizations and mitigates the risks posed by AI-driven attacks. This dual use of AI—both as a tool for attackers and defenders—highlights the importance of staying ahead in the cybersecurity arms race.

Preparing for AI Attacks

Preparation is key to defending against AI-driven cyber threats. Companies must invest in employee awareness training, regular security testing, and risk assessments to build resilience against potential AI threats. Additionally, having a robust incident response plan and utilizing AI-based forensic tools are critical for analyzing and responding to attacks. By adopting these proactive measures, organizations can better protect themselves from the evolving landscape of AI-driven cyber threats and ensure a swift and effective response when incidents occur.

EMPLOYEE CELEBRATIONS & SPOTLIGHT

Jonathan Gregg is a 2010 graduate of Glendale High School. Following graduation, he joined the US Air Force, serving in the Security Forces (Military Police), overseeing 50+ MPs and managing control center operations during multiple presidential details and high-risk base security operations.During his service, he was stationed in Alconbury, England and JB Andrews, MD. After his contract ended, Jonathan decided to leave the military to focus on family and put down roots, with the upcoming birth of his 1st son.

He transitioned to a role as an aerial cellular technician, building towers, changing equipment and testing signals at 100-700 ft. Following that, he became an Electronic Security Technician, installing alarm, camera, access control, and fire systems through central PA. Ready to focus on a new career path, Jonathan enrolled as a full-time student with SNHU, graduating Magna Cum Laude with a Bachelor's Degree in Cyber Security. Jonathan's degree allowed him to follow his heart into the IT field and to a position as Junior Project Manager with BSG, where he manages a variety of customer and internal projects as well as sales operations.

Outside of work, Jonathan enjoys spending time with his kids, watching football (as an avid Penn State fan), hunting, fishing, and cooking.

BSG IN THE COMMUNITY

BSG was proud to support the 16th Annual Puttin' for Panhandle mini golf tournament!

The tournament is a major fundraiser for Panhandle Home Health, and raises funds for the organization's charity care program. Congrats to all particpants!

SECURITY CORNER

Email Phishing

Cybersecurity is a critical aspect of modern digital life, aiming to protect systems, networks, and data from cyber threats. One of the growing concerns in this field is the use of artificial intelligence (AI) by hackers to enhance their attack strategies. AI-powered phishing, for instance, leverages machine learning algorithms to create highly personalized and convincing phishing emails. These emails mimic legitimate communications, making it difficult for users to distinguish between real and fake messages. This sophisticated approach increases the success rate of phishing attacks, posing significant risks to individuals and organizations alike.

Phishing emails are a common method used by cybercriminals to steal sensitive information such as passwords, credit card numbers, and personal identification details. These emails often appear to come from trusted sources, such as banks or well-known companies, and use urgent or alarming language to prompt immediate action. For example, a phishing email might claim that there has been suspicious activity on your account and urge you to click a link to verify your information. Once clicked, the link directs you to a fake website designed to capture your login credentials or install malware on your device.

To combat the threat of phishing emails, it is essential to implement robust cybersecurity measures. This includes using advanced security tools that employ AI to detect and block phishing attempts, educating employees and individuals about the signs of phishing, and promoting best practices for email security. Regular security testing and risk assessments can help identify vulnerabilities and improve defenses against phishing attacks. Additionally, organizations should have an incident response plan in place to quickly address and mitigate the impact of any successful phishing attempts. By staying vigilant and proactive, both individuals and organizations can better protect themselves from the evolving threat of phishing emails.

TECH TIPS & TRICKS

Tech Tips and Tricks for Microsoft Teams

Master Keyboard Shortcuts
- Quick Navigation: Use Ctrl + 1 to go to the Activity feed, Ctrl + 2 for Chat, Ctrl + 3 for Teams, and Ctrl + 4 for Calendar.
- Mute/Unmute: Press Ctrl + Shift + M to mute or unmute yourself during a meeting.
- Start a New Chat: Use Ctrl + N to quickly start a new chat.

Customize Notifications
- Manage Notifications: Go to Settings > Notifications to customize how and when you receive notifications for messages, mentions, and other activities.
- Quiet Hours: Set quiet hours to avoid notifications during non-working hours by going to Settings > Notifications > Quiet hours.

Use @Mentions Effectively
- Direct Mentions: Use @username to get someone's attention in a chat or channel.
- Team Mentions: Use @team or @channel to notify everyone in a team or channel about important updates.

Enhance Meetings
- Background Effects: Use background effects to blur your background or add a custom image by clicking More actions > Apply background effects during a meeting.
- Meeting Notes: Take meeting notes directly in Teams by clicking More actions > Meeting notes during a meeting.
- Live Captions: Enable live captions to see real-time subtitles during meetings by clicking More actions > Turn on live captions.

UPCOMING EVENTS

Dancing with the ARC Stars Event
October 19, 2024

We are a Silver Sponsor for this Fundraiser event where six dancers are raising money to help bridge the widening gap between state funding & programming needs for the ARC of Washington County.