Helion Issues New Warning to Auto Dealerships: Hackers Targeting Social Media Posts, Don't Click!

PRESCOTT, ARIZONA, UNITED STATES, June 12, 2017 /EINPresswire.com/ -- Helion Automotive Technologies, a leading provider of information technology (IT) solutions for auto and truck dealers, today issued a new data security warning for auto dealerships. Hackers are now planting malware inside of social media posts designed to lure employees of organizations to click on the post. If an employee takes the bait and clicks on the social media post, e.g. Facebook and Twitter messages and public postings, the malware is downloaded onto the employee's computer and may compromise the entire organization's network. Security software and firewalls cannot prevent this type of attack.

Helion Logo

"This is the same spear phishing scheme that hackers have been using successfully in targeted email messages for several years now," said Erik Nachbahr, President and CEO of Helion Automotive Technologies. "The problem is that although most employees have been told and know not to click on emails from people they don't know, they don't think twice when it comes to clicking on a message or offer in their Facebook feed. They are more trusting in a social media environment."

> This is the same spear phishing scheme that hackers have been using successfully in targeted email messages for several years now"
>
> *Erik Nachbahr, President, Helion Automotive Technologies*

Spear phishing is a type of attack that involves identifying specific people for attack, studying their social media posts to learn their interests and activities, and then creating a message or offer that appeals to them. For example, a recent breach at the Pentagon was caused when the wife of an employee clicked on a Twitter link that promised a great deal for a family-friendly vacation. She had previously been exchanging messages with friends over what they should do with their children over the summer. Although the wife was at home at the time, the hackers accessed the Pentagon employee's computer via a shared home network, and once the employee was back at the Pentagon, accessed the network from his computer.

Auto dealership employees are ideal targets for spear phishers looking to steal Personally Identifiable Information (PII) and bank account information.

Helion recently conducted a phishing test at an auto dealership by sending emails to 125 employees. Three employees clicked on the emails and were taken to a website where they entered their user names and passwords when prompted. If this was a real attack and customer information was compromised, the consequences for that dealership may have been thousands of dollars paid out in credit monitoring for customers, investigations and lawsuits.

"That test was a good sample that revealed auto dealerships are very vulnerable to this type of attack and need to do a better job at educating their employees," said Nachbahr.

To help prevent this type of attack, Nachbahr recommends the following tips:

• Educate employees to never click on links in social media posts and messages from their computers or personal devices while at work or at home. If they want to click on social media posts at home, encourage them to use a personal device that they do not bring into work.

• Require employees to change their network login passwords every 90 days. Encourage them to use strong passwords and to never share or give login information to anyone.

• Encourage employees to keep social media profiles private and don't accept friend or connection requests from people they don't know.

• If employees receive a phone call, email message or social media message from a banking institution, vendor, or other entity that asks for personal information, user names or passwords, do not give this information verbally or via email. Instead, contact the institution directly and give the information verbally. Also never click on a link that takes you to a website that requires login information; instead, open a new browser window and manually navigate to the website.

• Ensure that your dealership has the latest versions of security software and firewalls. Although they don't prevent phishing attacks, they can help to prevent other types of attacks.

• Every auto dealership should have cyber liability insurance, which covers costs associated with a data security breach and/or loss of data.

• Apply software updates, also known as patches, to Microsoft Windows, Internet Explorer and all software applications on every PC on a regular basis.

As the leading provider of managed IT services to auto dealerships nationwide, Helion offers 24-hour monitoring, managing and problem resolution for dealerships' computers, servers, and networks. Helion currently services more than 650 automotive and heavy-duty trucking dealerships, and 28,000 end users. The company handles an average 300 Help Desk calls every day and resolves more than 6,000 IT issues per month.

For more information on Helion's managed IT services, contact 443-541-1500.

About Helion Technologies

Helion...Putting Your Dealership in the FAST LANE! Helion Automotive Technologies is a leading IT solutions provider, providing auto dealers with faster, more efficient networks and secure data protection. From managed services to IT assistance and service desk help, Helion offers both short-term IT fixes and long-term planning so dealers can focus on what matters most: selling more cars. Helion has specialized in IT for more than ten years and works with 650+ auto dealers nationwide. Dealers can request a free assessment of their IT needs at http://www.heliontechnologies.com.

Holly Forsberg
602-680-8960
email us here
Carter West PR
