EBOOK

The Human Firewall

PROTECTING YOUR DEALERSHIP FROM CYBERTHREATS

HELION

CONTENTS

HELION

Introducing the Human Firewall

Cyberthreats are a major danger to auto dealerships. Hackers are driven by perceived opportunity, and they view independent companies, dealerships included, as potential victims of data breaches and theft.

This elevated level of risk means security must also increase, but the actual act of improving defenses may prove difficult. Purchasing new firewalls or updated anti-malware systems can only go so far. The most common and potentially damaging attack types used today involve social engineering and psychological tricks to sneak harmful content to employees. These phishing attacks turn human error into a major liability.

To stop phishing, dealerships need workers who are trained, educated and supported. With threats changing and evolving over time, training and preparation must be ongoing. This constant progress forms a human firewall.

The Threat of Phishing

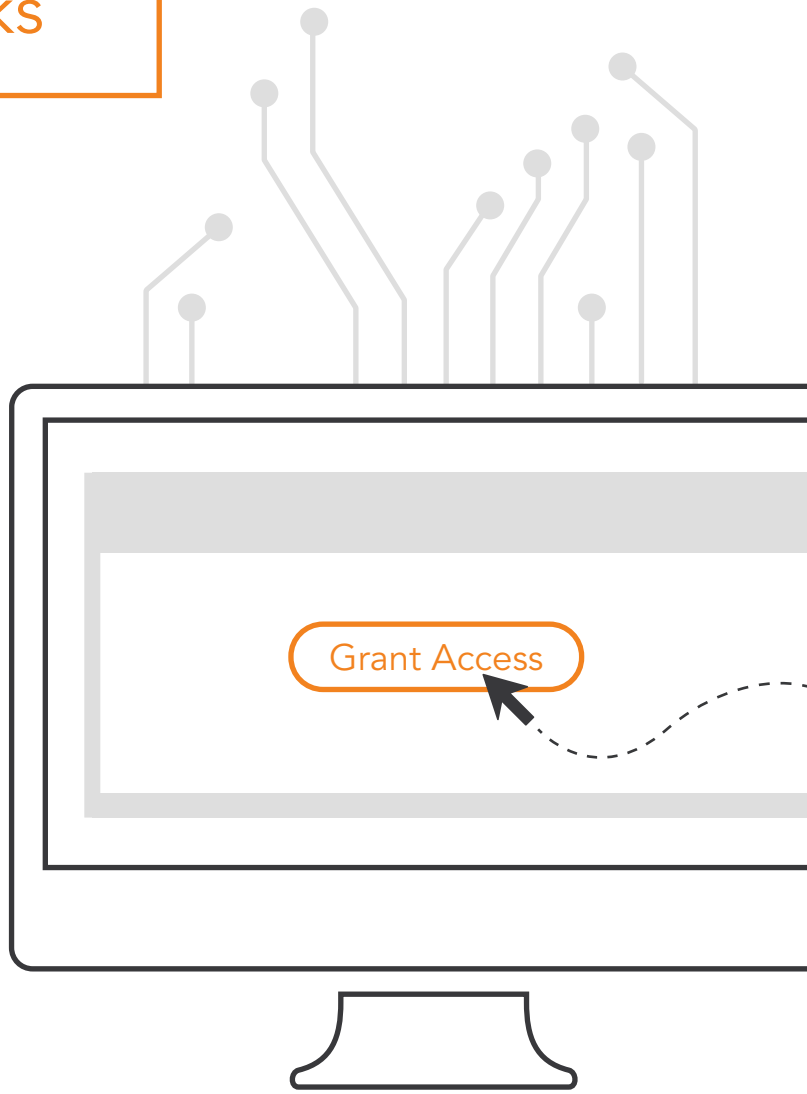
Social engineering attacks are often criminals' first choice, for a simple reason: They work. According to Cybersecurity Ventures research, **over 90 percent** of successful breaches begin with phishing emails.

Employees who aren't prepared to recognize and screen out phishing attacks enable this pathway for attackers, allowing them to get around defenses. When a worker clicks a link in a phishing email, enters personal information into a suspect website, or downloads dangerous files, an attacker gains direct access to internal data.

Further adding to the danger of phishing, hackers are becoming better at crafting these attacks, increasingly using precision tactics.

Advanced Social Engineering Attacks

In the old days, phishing emails were blasted to millions of recipients. These crude emails, full of misspelled words and suspicious-looking files, received occasional clicks, but would not fool most computer-literate employees today.



Unfortunately for businesses, phishing has changed since then. Cybersecurity Ventures stated **91 percent of "sophisticated" cybercrime** today begins with spear phishing. Criminals disguise their messages to look like they come from partner organizations or coworkers, making their schemes harder to detect.

In recent years, even more sophisticated approaches to data theft have emerged. For instance, last year cyberattackers initiated a sophisticated, widespread phishing scheme in which users were asked to grant email access permission to a Google Docs application. The application was a fake, and actually compromised their data.

Employees without proper training may be unprepared for such high-level attacks.

The Cost of a Data Breach

When data breaches occur, organizations are on the hook for large amounts of money. This provides a clear bottom-line impetus for companies to improve their defenses in any way necessary.

The average expense for a breached organization was $3.6 million.

The elevated cost of a data breach doesn't just come from a single factor. Companies that suffer these attacks have to repair the damage to systems, pay regulatory fines if their defenses weren't up to standards, notify victims whose information was lost, suffer reduced business due to declining customer trust and more.

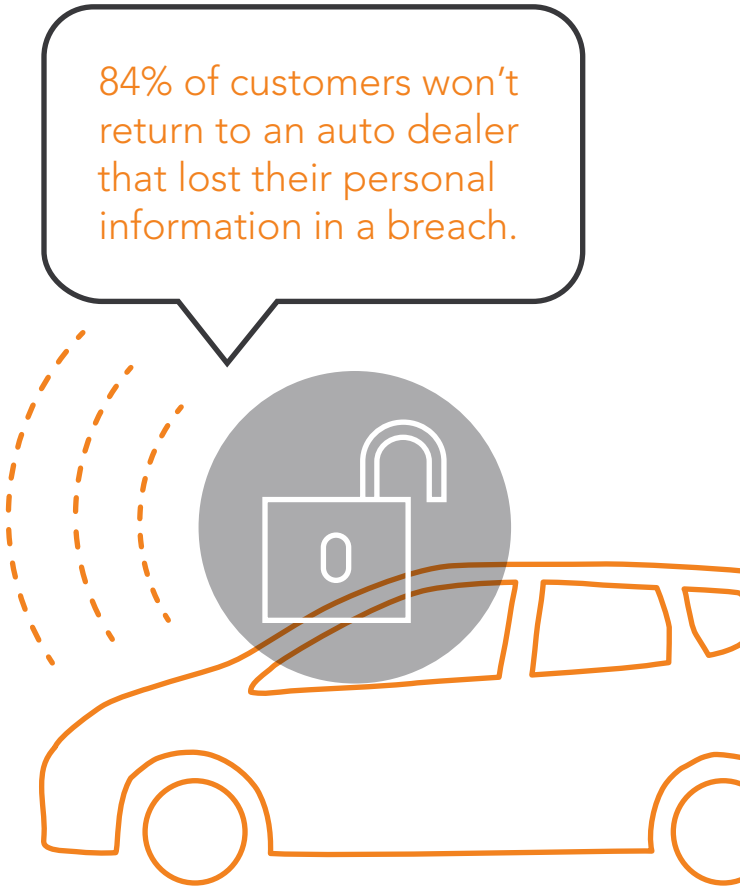
The Ponemon Institute's 2017 cost of data breach survey found the average expense for a breached organization was **$3.6 million**. The exact figure will vary widely depending on the scale of the incident – Ponemon **put the cost of each lost record at $141**.

Lasting Damage Due to Data Loss

Dealerships may suffer extended and highly damaging losses from a data breach, well beyond the initial costs. Perception of these businesses may change for the worse and, in an era of unparalleled customer choice, they can't afford negative perception.

A Total Dealer Compliance Survey indicated **almost 33 percent of consumers have doubts about data security** when they go to a dealership to purchase a vehicle. Additionally, 84 percent of customers won't return to an auto dealer that lost their personal information in a breach. Loyalty and repeat business are essential parts of any dealer's income, and so losing existing customers' trust can be financially devastating.

Unfortunately for dealerships, many companies in the automotive field aren't prepared to face the escalating threat of cybercrime.



Dealerships are Vulnerable

Auto dealerships are primarily brick-and-mortar concerns, even in this increasingly digital retail age. It's unfortunately common for dealers to lack advanced IT departments, instead relying on limited personnel mostly dedicated to solving simple problems with internet infrastructure and other day-to-day worries. These teams aren't equipped to give the kind of training that will keep their co-workers safe from phishing and other advanced cyberattacks.

The TDC survey noted **only 30 percent of dealerships have a network engineer** who is trained and certified in computer security. Furthermore, over 70 percent of dealers don't have updated anti-virus software.

70% of dealers don't have updated anti-virus software.

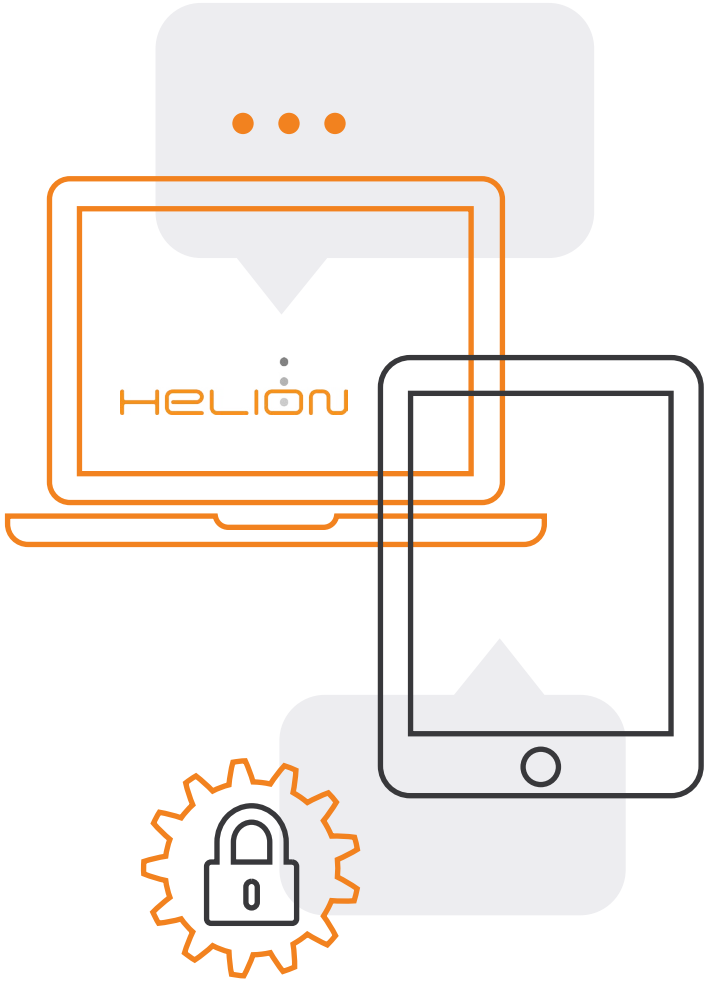
Dealerships Must Step Up Defenses

Without the presence of in-house employees who understand the threats associated with modern phishing and related attacks, it's difficult for dealerships to protect data. This is reflected in the relatively high percentage of consumers worried about handing over their data.

Due to the fact that auto dealerships handle consumers' financial data when they arrange payment for their new vehicles, these companies are heavily regulated by government agencies.

The combination of demanding expectations from customers and federal authorities with largely undeveloped IT capabilities is untenable – dealerships are at elevated risk of suffering data breaches. It's up to auto industry leaders to resolve this situation. Bringing in third-party assistance is a potential solution, but leaders have to ensure they're working with the right companies.

Receiving Training from Helion



While TDC found almost 85 percent of auto dealerships are working with third-party IT service providers, not all of these partner organizations are equal.

Helion understands the nature of security in the modern automotive workplace, and therefore we know security procedures must go beyond digital countermeasures. Helion is the largest managed IT service provider focusing specifically on the needs of dealerships. In addition to monitoring and updating important IT protective services, Helion offers security awareness training and simulated phishing services through a partnership with KnowBe4.

This type of training builds upon the weakest links in the typical dealership's security posture – worker awareness and preparedness. When employees understand how to recognize and defend against social engineering attacks, they become the human firewall these organizations need.

KnowBe4 Features

Working with KnowBe4 means getting the best possible preparation and education for employees. Not only do team members receive up-to-date training on the types of threats to be aware of and avoid, but there are practical features that provide more in-depth education.

Monthly tests send fake phishing emails to employees to determine whether they are learning to spot the signs of suspicious messages.

A full library of video training content, interactive gamified modules and online interactive solutions to provide advanced education.

A phishing alert button in employees' email client allows them to easily report dangerous messages.

Benchmarking features compare a dealership to other companies in the industry and determine whether security is improving.

Advanced reporting makes it clear which employees are most prone to risk and require further instruction.

Protect Your Dealership

Dealerships are some of the most vulnerable companies from a digital security perspective. Despite high consumer expectations and government oversight, there is a general lack of IT know-how among internal staff. This is a risky combination, and it calls for immediate resolution. Even one breach could be hugely costly, reaching levels of long-term expense that may prove devastating to independent dealerships' ability to stay open.

The key to digital security is to focus on the human element, turning the auto industry's greatest liability into a point of strength. Helion's security offerings, partnered with KnowBe4, provides the necessary employee education. This newly prepared workforce is the human firewall, a great asset for any dealership.

Reach out today to learn more about this essential part of defending your dealership.

HELION

heliontechnologies.com

1965 Greenspring Drive
Timonium, MD 21093

443-541-1500