

# Hack Attack

Treat your customers' data like you would your family's.

From Ashley Madison to Target and Sony, we've all seen the headlines about cyber hacking into databases – and the unfortunate fallout. Those organizations are still reeling from the impact, and trying to regain the trust of the customers affected by the breach.

Over the past two years, it's estimated that the average data breach has increased by 23 percent. In a dealership, your business focuses on vehicles, which means data security may not be top of mind.

But it should, if only because the F&I office contains very sensitive data like credit card numbers, income records, social insurance numbers, driver's license numbers and just about every piece of information needed to take a person's life hostage. When customers provide their private information, they're placing a great deal of trust in you and your store. You want to ensure that you maintain that trust with the respect it deserves, and treat their data with the same care that you'd treat your family.

Although many F&I offices are taking steps to protect their data, it may not be enough. That simple firewall that was satisfactory a few years ago may not provide as much protection as it should.

## Encryption

For example, how does your store deal with credit card information? How long is it kept on file? There's usually no good reason to keep credit card numbers in the system for any reason.

Ensure that your systems are encrypted. If you're dealing with a major DMS supplier, chances are the software is already encrypted. That simply means that the data is scrambled when it's stored, so without the proper code, it simply comes up as indecipherable nonsense. If you're not sure, check with your supplier.

Studies show that the majority of data breach incidents happen due to employee negligence, such as clicking

the office just get an interesting phishing email, talk about it. Make an image, share it around the office. What are the issues? How can you tell if an email is for real? Spread the word, and encourage others to contribute their two cents. Get your team engaged, and help them understand it's everyone's job, right up to the front lines. When everyone's participating, on the same page and protecting the store, hackers will have a harder time of it.

## That benevolent gesture of donating your old equipment to charity can backfire if the machines and all their accessories are not suitably cleaned of data!

on email links that have malware embedded in them. So the F&I manager needs to take a leadership role, and become the subject matter expert. Make security and privacy training a priority, and lead by example.

Open up the lines of communication about security, and start conversations to raise awareness. Remind your team not to leave sensitive files on their desks, and develop a process where they are properly stored. Don't put private data on unprotected USB drives or share it in an email, unless totally necessary.

Security is more of a journey, not a destination. Should a breach make the headlines, or should someone in

## Common sense


But many data breaches aren't necessarily high tech. Often, it can just be a matter of using common sense to mitigate the chances of data falling into the wrong hands. Are there laptops or other mobile devices with sensitive information that can "walk" away? Do documents get thrown in the trash or recycling, where they can be retrieved or blown down the street on pick-up day? Or are they shredded and disposed of properly?

Old hard drives on computers, printers, phones and servers should be wiped clean before they are discarded. That benevolent gesture of donating your old

equipment to charity can backfire if the machines and all their accessories are not suitably cleaned of data!

Sharing passwords and user credentials should be discouraged, and that includes the IT person. They shouldn't need a password to access your device, if they are already on the system. And while it's tempting to provide a password to a colleague if you're in the middle of something while they need access to a file, this is one instance where sharing is not caring. Once you provide that information, you lose accountability, since it can be passed on around the organization like a virus.

In fact, it's a great idea to change passwords on a regular basis, whether or not you've shared it with anyone. If someone has your password, they can use it to impersonate you and even make it look as if you were the perpetrator of a hack. Don't use birthdays or commonly known information to compose a password, use something that's very specific and private to you, and include letters, icons and numbers that mean something to you – but not anyone else.

So while technology plays a huge role in data protection, those tools are only as effective as the individuals using them. Common sense, communication and education are equally, if not more important, to ensure that the valuable data in your system remains accessible only to those who have earned the right. You don't have to spend a lot of money on expensive tools, but rather, educate those who are using your F&I department's technology.  *Krystyna Lagowski*