Keep Your Customers Close and Their Data Closer

It’s not just a problem for the likes of Equifax. Today, businesses of all sizes face an array of potential attacks from digital burglars. Timothy Swift, a cybersecurity expert from Saint Joseph’s University, explains how small- and medium-sized businesses can keep their digital systems safe from attack.

NO PHISHING ALLOWED
It can happen to all of us, so get your virus protection in order.

One of hackers’ most effective tools to get malware and viruses onto your computer is called phishing, where hackers send an email that looks like it’s from a company or person that you know. When a link is clicked in the email, it opens the door for whatever viruses the hacker is looking to install, whether they want to steal data, monitor activities or even take over your system. Avoid clicking on outgoing links unless sure of the email’s origin, and have safeguards. Even baseline virus protection alerts the user when a virus program activates. Consider software that has a remote encryption feature. That way, if the laptop is physically stolen, there will be no way for the thieves to see your information.

HAVE A FALLOUT PLAN
Back that data up, preferably to a cloud-based system.

“The most common weapon used to attack small businesses is a particular type of malware called ransomware,” Swift says. You’ve probably heard of high-profile hacks where large corporations have their information distributed publicly. But for lower-profile businesses, the more common threat is simply not having access to critical data. The hackers lock down computers and threaten to permanently wipe out data — passwords, customer information, financial records — until a ransom is paid. However, it doesn’t matter if they won’t let you access your data if you have it somewhere else. Best practice is to back up your data to a cloud-based service that guarantees data availability.

CUT OUT THE MIDDLEMEN
If a public network seems too good to be true, it just might be.

Hackers may not even need to hack you to get your data, thanks to something called a man-in-the-middle attack, which can occur whenever an employee hooks up to an unsecured wireless network. Everyone’s been there: Waiting for a flight, you see a network labeled Airport WiFi Official, and you log in to check your email. Unbeknownst to you, the network was set up by a hacker. “That’s some dude sitting at that terminal, picking up every single keystroke,” Swift says. By the end of the session, they’ve got passwords to all of your accounts. Stick to password-protected WiFi networks, especially when using a work account. Two-step verification can also protect accounts even when passwords are stolen.

Saint Joseph’s University cybersecurity master’s and certificate programs expose students to the most recent IT technologies and methodologies that strengthen the security and resilience of cyberspace. Students from diverse education backgrounds are welcome to apply to the online program. Learn more at sju.edu.