Cyber Security and Online Bill Payments: Protecting Yourself from Theft and Fraud

Paying bills online for shopping and services has never been easier with small businesses now using credit card processing, which eliminates any friction when doing transactions. However, this convenience doesn't come without a cost.

Credit card fraud and identity theft is now on the rise. While the official records released by the Federal Trade Commission report that the cases of identity theft in the US peaked in 2015, the numbers are rising back again – up by 14.85% from 2017 to 2018. Almost a third of these are credit card fraud committed on unsuspecting consumers. Businesses caught in these controversies not only risk hefty fines but also risk losing potential revenue and their customers' trust.

While most of the media's attention has been on large-scale attacks and data breaches that affect huge companies, Verizon found that 43% of cyber attacks are directed at small businesses. Another study found that these breaches are draining at least $200,000 from businesses of all sizes. While this may sound like a small price to pay for large enterprises, it can be devastating for smaller businesses. Coupled with the increasing shortage in cybersecurity professionals, which Maryville University believes to be nearing 3 million globally, cyber-attacks pose an acute peril to both businesses and consumers. That's why efforts to secure your transactions should be both business- and consumer-driven.

How do they steal credit card details?
A whopping 3% of all credit cardholders in the US experience fraud from online transactions — or what officials call card-not-present fraud cases. In fact, your customers can be victims of credit card fraud without you knowing about it. But how do these attackers do it?

Data breaches. There's been no shortage of headlines pertaining to data breaches last year. With huge online retailers like Macy's, Hyvee, and Poshmark, to name a few, being compromised by data breaches in the past, there's a good chance many users' card information is just out there for the taking. In fact, a Gemini Advisory report revealed that more than 30 million credit card details that were tied to last year's breach on convenience store company Wawa were being sold online. The organization is now facing a wave of class-action lawsuits directed at their alleged failure to protect customers' information.

Malware and viruses. While online bills payment is becoming more secure, hackers continue to use malware and viruses to get credit card information. E-skimming, a type of malware that infects checkout pages to steal payment and personal information, is now on the rise and has affected websites of all sizes. Similarly, a study by the University of Cambridge in England and Sweden's Linköping University discovered a malware that can guess your credentials just by listening to how you type.

Mitigating the cyber-risks of online bill payments

So, how do you secure your business' and your customers' financial information?

1. Train your employees against cyber-risks. As mentioned above, the high demand for cybersecurity personnel means that not all businesses, especially smaller ones, can have a dedicated IT department against fraud. But training your employees to be vigilant against and even identify attacks can go a long way. In fact, this is a standard requirement to comply with PCI security practices set to increase your employees' security awareness.

2. Patch your site and software. Sites that fail to maintain codes and unpatched software are a hackers' paradise. Make sure you have an SSL certificate and TSL encryption to keep the low-level hackers at bay. In addition, be up to date with the software patches your vendors' issue.

3. Only use trusted payment processing providers. The payment industry has made strides in introducing advanced, risk-based decision-making standards and protocols for businesses in the past few years – effectively mitigating most of the outdated schemes. Standards like EMV has eclipsed outdated and unsecured methods of the past. Only deploy secure online payment processing services that use trusted and up-to-date payment processing methods.

4. Report suspicious activity immediately This can't be said enough: closely monitor your transaction history. If you find any issue with your credit transactions and online bills, call your payment provider or bank directly.

Piece especially was written for IntelliPay.com

by Janae Brayden