This article was published by Fortune Magazine on December 15, 2014

'Tis the Season to Protect Your Credit

The likelihood of having your data compromised goes way up during the busiest shopping days of the year.

'Tis the season . . . for cyber-breaches, identity theft and a big percentage of the annual losses that run to nearly $25 billion from those crimes in the U.S. alone. U.S. retail websites were attacked 547 times per day during the last holiday season, according to Imperva, which reviewed data from November 14, 2013 to January 9, 2014. That's 264% greater than the average of 150 attacks per day in the four weeks prior to November 14, and 104% greater than the average of 267 attacks per day in the four weeks following January 9. And that represents only three of the most common types of attacks.

So what can you do about it? Try following a few broad, practical principles to guide your behavior:

Rely on a single credit card. For online and in-store purchases, use a single major credit card if possible. This makes fraud detection easier, since your buying patterns are concentrated in a single system. More than that, most issuing banks indemnify you against losses in the event of fraudulent charges. Your credit card also isn't as vulnerable as your debit/ATM card, which can be used to empty your bank account, even if your PIN number hasn't been compromised, or even if you process it as a credit card. Even though banks will help you recover, the hassle is greater for debit than credit theft. In fact, to be entirely safe, use your debit/ATM card only at your bank's own ATMs.

Create better passwords and a quasi-faux email account. The most security-minded companies put layers and layers of protection – what they call "defense in depth" – between themselves and evildoers. You, too, can create these buffer zones — not just with up-to-date firewall and anti-virus software on your devices, but also through other means like password manager applications. You can't rely on online websites to keep your passwords secure, and you need a unique and strong password at every site you use. Password manager apps make it easy for you to maintain all of those strong passwords and require you to remember only your master password. And that master password can be an easy-to-remember sentence or phrase, which actually takes longer to crack than a complex word. (For instance, "Pa55w0rd" satisfies most rules, but it is easy to crack versus, say, "ithinkmypetisthegreatest.")

Also, because you're more likely to create new accounts on websites and sometimes at physical stores during the holiday season, it is a good time to add yet another layer of defense by using a "throwaway" email account. First, create a new email account that is distinct from the account you use for all of your important personal or professional correspondence. When registering for the new email account, leave all personal information empty, or fill in imaginary data. When you open a new in-store or online account, direct all correspondence to the new email account. Use that email account only for that purpose, and don't send any emails from that account. If this account is compromised, there is no address book to bug your friends, and minimal personal information to steal.

Take advantage of all available protections. At brick and mortar stores, for instance, if your credit cards have that gold square patch on the front, it means it is already equipped as a "smart card." Most major credit card issuers in the U.S. have announced that fraud losses will shift to retailers who have not installed smart POS payment terminals by October 1, 2015, which read this gold patch on your card as an extra level of protection. Many major chains, including Wal-Mart WMT -1.17% and Kroger KR -0.05% , already have activated their checkout systems to work with these smart cards – so ask at the checkout counter if that slot at the bottom works, instead of swiping the magnetic strip along the top or side. Using it may take a few extra seconds at checkout, but you are taking early advantage of the new level of protection against theft, fraud and the inconvenience of replacing your card – not to mention reducing the risk of as much as $100 of any fraudulent transactions, which some card issuers require of cardholders. Before using any form of payment, whether it's a store-branded credit card or one of the new "contactless" mobile payment systems that allow you to pay by waving your cell phone at the POS terminal, make sure you know whether the user agreement indemnifies you against losses. But if you're like most people, you don't have the patience to wade through those interminable and often impenetrable agreements. You don't have to – a quick online search should turn up a succinct answer to the question.

Glenn Kapetansky is Chief Security Officer for Trexin Consulting a management and technology consulting firm specializing in the application of advanced technologies.