

Tips for Keeping Your Information Safe During the Holidays

1. Buy Only from Reputable Retailers. While counterfeit goods are often hard to spot, they are common out in the marketplace – especially online. Many items sold by unknown merchants turn out to be counterfeit or resold stolen goods. Consumers should exercise caution when merchandise is priced well below the going commercial rate.

2. Take Extra Steps to Secure Online Purchases. While EMV chips safeguard card data at the point of sale, they don't protect e-commerce sales. There are alternative payment methods that are safer to use online and via mobile devices, such as prepaid debit cards, Visa Checkout, Masterpass, and tokenized payment options like Apple Pay.

3. Secure PCs and Mobile Devices. One of the most problematic security threats to holiday shoppers is located right in their homes: the personal computer. You may be shopping from laptops, PCs and mobile devices infected with viruses and malware that give cybercriminals direct access to their personal and account data. Be sure to install quality virus and anti-malware scanning software on all computing devices to keep data secure.

4. Beware of Instant Savings Discounts. Consumers are often barraged with quick credit offers that can lead to ancillary identity theft. You need to pay close attention to how your information is being collected if you are asked to open a credit account in exchange for a discount. Avoid verbally providing information to sales people, and you should use caution as well when filling out paper forms that can easily be pocketed by retail personnel after they have left the premises.

5. Don't Trust Those "Knuckle Busters." Old-fashioned imprint machines that produce a carbon copy of payment cards still exist in the marketplace. Don't ever use one.

6. Don't Swipe at Checkout, Either. Chip-enabled payment cards are protected by very powerful fraud-fighting properties. The magnetic stripe on the back of the card is much less secure, which is why members should always avoid "swiping" their payment card at checkout. If a retailer has a valid reason for not accepting chip card payments, you should ask to use Apple, Samsung or Android Pay instead.

7. Keep a Close Eye on Balances. Keep a close eye on your checking, savings and credit card accounts, and know how much money you have on deposit, and also track how much you owe on revolving charge accounts. If dramatic changes in balances are noticed, you should contact the credit union immediately.

8. Use Mobile Controls and Alerts. Fraud continues to rise – and is even more prevalent during the busy holiday shopping season – which is why it is so important for all consumers to play an active role in their own card security. Download our [FREE mobile app](#) to access your account(s) 24/7 and the [FREE CardNav app](#) for your debit card controls and alerts which allows you to monitor transactions, restrict purchases to certain locations, merchants, merchant types and time periods. You can also turn your debit card off altogether when not in use.

Bottom Line: Don't let fraud steal your holiday cheer.

**Contact the Tobacco Valley Teachers Federal Credit Union at
860-253-4780 or 800-749-8305.**