Safeguard™

The Grinch Effect:

7 Holiday ID Theft Prevention Tips

GTN2GEWP

This month officially kicks off the holiday shopping and celebration season. It is a time for joy, giving and togetherness as well as a wonderful time of year to honor those we care about.

Unfortunately, the abundance and financial richness of the holidays also attracts scammers and data thieves who take advantage of this distracting season. I call this **The Grinch Effect – manipulating or stealing from innocent people while they are busy celebrating.** Like the Grinch pilfering the last stockings from the fireplace, identity thieves exploit your distraction and pluck pieces of private data from homes and office parties, shopping malls and online transactions.

Unlike the Grinch, however, fraudsters don't have a last minute change of heart in response to the underlying goodness of mankind. They rob you blind, carry their spoils to the top of Whoville Hill and move on to the next unsuspecting victim. To make sure that you, your family and your business are not the next ones targeted, use these 7 Holiday Identity Theft Prevention Tips.

7 Holiday Identity Theft Prevention Tips

1. PROTECT YOUR HOME AND OFFICE

   Holiday parties, at home or at work, are a major source of data theft. Opportunistic identity thieves are looking for smartphones, iPads, financial documents, checkbooks, credit cards, disks, laptops, client lists, thumb drives, sensitive trash or mail, purses, wallets and all other sources of identity. Not only do the devices have face value, but the data on them is a veritable gold mine. Ignore the voice of denial demanding that your friends, family, co-workers, vendors, customers and colleagues wouldn't possibly steal from you. I hear hundreds of stories each year at my speaking engagements with the same sad ending — the victim knows the thief! Don't assume the worst about your guests,

> *"Ignore the voice of denial demanding that your friends, family, co-workers, vendors, customers and colleagues wouldn't possibly steal from you."*

simply protect yourself. Statistics suggest that identity theft is committed by someone the victim knows approximately 30% of the time.

SOLUTION

Just before a holiday gathering, **centralize all potential sources of identity into one secure location** (like an office with a locking door). When a potential thief disappears upstairs (a friend's sketchy date who wants to "see the house" or a caterer moonlighting as a scammer), you don't have to worry about it. When the high-traffic season is over, return your house to normal; unless you regularly use a cleaning service or allow outsiders into your home. If you are a guest in someone else's home, leave your valuable data at home or in your trunk.

2. STOP DEBIT & CHECK FRAUD

When you use a debit card, the money is drawn directly from your bank account. If fraud does occur, it's harder to get the money reimbursed. More importantly, while the issue is being resolved, you don't have the money to spend. In addition, debit cards generally only reimburse fraudulent purchases if you catch them within 30 days.

SOLUTION

Instead of paying with (or even carrying) your debit card, **use a credit card or High Security checks.** When you use a credit card, nothing is withdrawn from your bank account. In addition, credit cards generally give you a longer period (90 days) to catch the fraud before you are held liable. If you need to pay by check, make sure you use High Security checks that have visible fibers, true watermarking, thermochromic ink, full-feature hologram (like on credit cards) and protection against multiple chemical alteration agents (not just

fingernail polish remover). Sign your checks with a gel-based pen that cannot be easily dissolved.

3. PROTECT YOUR IPAD, SMARTPHONE, LAPTOP AND PURSE

Malls, stores, restaurants and cafes are exceptionally busy places during the holidays. This breeds a perfect environment for thieves to make off with your goodies while you shop, dine or relax. It only takes a second to pick up a purse or briefcase when you go get a refill.

SOLUTION

Leave your identity at home. Consider taking only your driver's license and one or two credit cards with you shopping. Put your credit cards, license and cell phone in your front pockets. Take a break from your digital devices, briefcase and purse for the day. Your risk decreases exponentially when you leave more at home. If you must have a purse, use one that zips and hangs in front of you or consider using a backpack. As a last resort, hide your devices in the trunk **before** you park. Parking lots are commonly monitored by thieves looking for valuables left behind.

"Although you may trust the baristas at your local coffee shop, you can't always trust the person sitting next to you. Hackers can easily tap into Wi-Fi connections ..."

4. STOP SHOPPING ONLINE USING PUBLIC WI-FI HOT SPOTS

Although you may trust the baristas at your local coffee shop, you can't always trust the person sitting next to you. Hackers can easily tap into Wi-Fi connections at public hot spots to steal your identity information. This can be especially dangerous when you are making purchases with your credit card on unsecured connections.

SOLUTION

If you must shop online while out in public, **enable tethering on your smartphone.** Tethering connects your computer to the Internet using a smartphone (or Internet-enabled cell phone). It increases security because the mobile transmission between your cell phone and the cell tower is encrypted (scrambled) and hard to intercept. Therefore, when you use your smartphone to surf the Web, you are accessing a protected connection. The connection may be slower than a traditional Wi-Fi hotspot, but it is much safer. Call your wireless provider and ask them if your smartphone has tethering capabilities. This solution should be about $15 a month. Make sure that you shop on reputable websites, not just those with the cheapest prices.

5. WATCH OUT FOR HOLIDAY SCAMS (ESPECIALLY ON FACEBOOK & EMAIL)

Because you tend to be more giving during the holidays, scammers target you during this time of year. Whether they are asking for a donation to a charity, promising free iPads, claiming to be a friend in need or are asking you to click on something outrageous or out of character, don't fall for it.

> *"If a friend sends you a link that seems out of character, delete it as their account may have been taken over by scammers."*

SOLUTION

Follow these simple rules: **Never transact money based solely on a wall post,** email or phone call. Only donate to known charities and only when you have initiated the gift. Respond to charity requests by directly contacting the charity. If a friend sends you a link that seems out of character, delete it as their account may have been taken over by scammers. In addition, don't post holiday vacation plans online, as this is an easy way for a thief to know exactly when to rob your home.

6. CATCH ACCOUNT FRAUD QUICKLY

Sometimes there is no possible way to prevent identity theft. The reality of living in the information economy is that your identity will occasionally be compromised. But don't worry. If you catch fraud quickly, you won't lose much.

SOLUTION

Most types of holiday identity theft can be caught by frequent **monitoring of your checking, debit and credit card accounts.** Remember, the pain of this crime gets much worse if you don't catch it quickly. By keeping an eye on your financial statements, you can catch credit card and check theft immediately. Sign up for automatic account alerts to quickly and conveniently notify you when transactions occur. If you receive an email for an amount you didn't spend, BINGO! You're probably a victim of fraud. Visit your bank and credit card providers online to set up account alerts. For added protection, sign up for an identity theft monitoring service that helps you detect all types of cyber fraud.

7. PROTECT YOUR BUSINESS

Many businesses spend a great deal on technology (laptops, smartphones, servers, iPads, networks, DSL) but very little on protecting those powerful tools. This weakness is the most dangerous link in the data breach chain.

SOLUTION

This holiday season, give your business the gift of a security audit. **Invest in a technology audit firm to help you fix your major vulnerabilities.** Have them review your default firewall settings, password strength, backup and recovery procedures, Wi-Fi encryption scheme, user-level access controls, remote-data wiping capabilities, operating system patches, automatic security updates, anti-virus and security monitoring software

and any other customized security you need to implement. Spending a few dollars before a breach happens could save you thousands of dollars recovering from identity theft, data breach or corporate espionage.

None of these tips are overly time consuming, and only the last one requires a significant investment. Don't wait until the New Year to start, because unlike the Grinch, most identity thieves don't return your belongings at the end of the day. Happy Holidays!

John Sileo lost almost a half-million dollars, his business and his reputation to identity theft. Since then, he's become America's leading keynote speaker on identity theft, social media exposure and weapons of manipulation. His clients include the Department of Defense, Pfizer and Homeland Security. To learn more, visit ThinkLikeASpy.com or contact him directly at 800.258.8076.