Preventing Holiday Identity Theft Scams

MINIMIZING YOUR RISK OF FRAUD DURING A TIME OF INCREASED TRAVEL AND SPENDING

December 2017

GENERALI GLOBAL ASSISTANCE

In partnership with the Identity Theft Resource Center

PRESIDENT & COO, GLOBAL IDENTITY PROTECTION SERVICES
GENERALI GLOBAL ASSISTANCE (GGA)
Paige L. Schaffer

PRESIDENT & CEO
IDENTITY THEFT RESOURCE CENTER (ITRC)
Eva Velasquez

CONTRIBUTORS
Nikki Fiorentino, ITRC
Kelly Dwyer, ITRC
Alex Hamilton, ITRC
Karen Barney, ITRC
David Brown, GGA
Megan Dwoskin, GGA
Laurel Laluk, GGA
Julie Yoo, GGA

CONTACT
Eugenia Buggs
VP, Global Marketing, Identity Protection Services
Generali Global Assistance
4330 East West Hwy Suite 1000
Bethesda, MD 20814
240-330-1091
eugenia.buggs@us.generaliglobalassistance.com

INTRODUCTION

The holidays are a time of reconnection and generosity—and a rush to shopping malls and e-commerce websites, resulting in increased spending and retail exposure. The holiday shopping season seems to grow longer each year, with some companies beginning their advertising in October and continuing through the post-Christmas clearance sales. Black Friday, Cyber Monday and Small Business Saturday, following Thanksgiving, are days when you can score some of the best deals of the year while witling down your holiday shopping list. Unfortunately, these days also bring with them risks of data breaches and identity theft.

The 2013 Target data breach spanned the entire month of November and resulted in more than 41 million customers' credit and debit card information being stolen via the retailer's infected point-of-sale system. This single event sparked one of the first national conversations about cybersecurity, data breaches, and fraud or scams.

Since then, the U.S. has continued to face a record-setting number of data breaches, compromised records, and consumer fraud complaints. These widespread, and often complex, forms of attack can overshadow the more mundane everyday scams targeting you which can be just as, if not more, devastating. These more common scams continue to cause serious financial and emotional hardship for people year after year by exposing their personal information and potentially exacting fraudulent transactions.

The damage these scams cause is very real, yet knowledge of these types of crime is limited amongst the public. According to a survey conducted by the AARP, 70 percent of U.S. holiday shoppers failed a short quiz about how to stay safe from holiday scams. Likewise, many of the respondents reported engaging in behaviors that put them at risk of falling for various holiday scams such as: donating to suspect charities without confirming important details, purchasing gift cards from potentially risky locations, using debit cards that offer less consumer protections, using unsecured public Wi-Fi, or shipping and receiving packages without signatures. Even though consumers are not knowledgeable about how to protect themselves or how these crimes often work, they are concerned. A recent survey shows that 91% of Americans are skeptical that businesses are doing all they can to protect the personal and financial information of their customers. The survey also shows that 75% are concerned about having their personal information compromised in a data breach.

Now more than ever, everyone needs a better understanding of how to protect theselves from scams. This is especially true during the holiday season when the risk of fraudulent activity sharply increases, and stress levels are high.

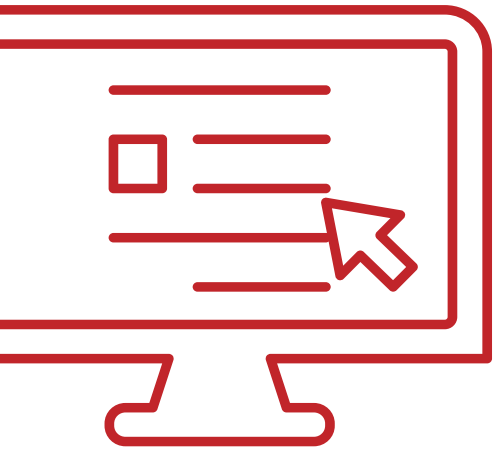
Throughout this paper, we will introduce you to the most common scams that transpire during the holidays. You will also find tips you can use to minimize your risks not only during the holiday season but throughout the entire year.

CONTENTS

ONLINE RETAIL SCAMS

One of the most common scams during the holidays exploits online shopping. With reports showing that 75% of Americans plan on doing their holiday shopping online this year, we need to be even more alert to scammers and their tactics.

A man from Indiana spotted a deal he couldn't pass up on Craigslist for a used truck. In order to purchase it, he needed to send the seller $2,000 in Amazon gift cards, which were quickly drained by the scammers. He learned it was a scam after he received an email from the seller asking to send more money.



THREATS

- **Spoofed Websites:** The fake websites mimic popular websites, especially e-commerce sites, and are designed to deliver malware to your computer, or steal credit card information or personal information. They are often supported by fake social media advertisements to drive traffic.
- **Counterfeit Products or Websites**: These scams involve fake websites selling counterfeit products for very cheap. Victims may also find that a site pretends to have the top holiday item for sale, but it's really just a ploy to steal money from the victim.
- **Shipping Scams:** The scams can involve spoofed emails that encourage the victim to click on a link to see why their item is delayed or payment scams that claim their item is not arriving until the rest of the "overdue balance," is paid.

PREVENTION TIPS

- Check the website address for misspellings and type the URL directly into your browser instead of clicking a link from an email or social media site if you are unsure the business is legitimate.
- Search online for the vendor's name and use the words "scam," "complaint," or "review" to glean more information about the business. You can also search the name of the company on the Better Business Bureau's website.
- Make sure there is an "s" at the end of "http" in the web address before entering credit card information or personal information. The "s" stands for a secure connection and can help reduce the chance of falling for an online scam.
- Refrain from purchasing anything while on public Wi-Fi, since these type of connections are often unsecure and can be more easily hacked. It's safer to use your cellular connection or a VPN (Virtual Private Network) to prevent others from seeing what you are doing online.
- Use credit cards instead of debit cards since they often offer more fraud protection.

SEASONAL EMPLOYMENT SCAMS

In 2016, the Better Business Bureau's Scam Tracker highlighted 39 different cases of seasonal employment scams. Many of these scams began with an unsolicited job offer via email which should serve as a red flag throughout the year, but especially at the holidays.

THREATS

- **Employment Offer Scam**: Many employment scams are nothing more than phishing attempts to get applicants to turn over their sensitive information, like birth dates and Social Security numbers. They sometimes come with the promise of "easy money" or a work-from-home opportunity that requires little or no activity. Once the victim has accepted the position, their personal information is stolen, and they never hear from the "employer" again.

- **Reshipment Scam**: A fake employer "hires" an employee to receive stolen goods or payments and then sends them on to someone else.

- **Overpayment/Fake Check Scam**: The victim is informed that they were overpaid for work completed. The victim is then instructed to deposit the check, keep the amount owed, and wire back the difference. When the fake check is deposited, the funds appear to be available within days before it eventually bounces, causing the victim to lose the money and face cosequences from their financial institution.

PREVENTION TIPS

- Be suspicious of overpayments. A check can bounce even after your bank allows you to withdraw cash from the deposit. Even if a bank representative tells you that a check has "cleared" it could take weeks to bounce.

- Never send money to people you don't know, especially if they ask for the money in an unusual form such as wire transfer or prepaid debit card. Likewise, do not share personally identifiable information such as date-of-birth, bank or credit card accounts, passwords, etc. with anyone you do not know. Think twice if you are asked to pay for any services (background checks, drug testing), pay in advance, get hired without an interview or are asked for personal information before you are hired.

- Look for typos, misspellings and vague information about the company in the job posting.

CHARITABLE GIVING SCAMS

Identity thieves have been known to take advantage of the season's goodwill by creating fake charities to solicit donations fraudulently. These scams can be more difficult to detect because the thieves will often use a name that closely resembles that of a reputable organization and employ common fundraising tactics such as phone outreach, face-to-face contact, email, or social media.

THREATS

Signs that a charitable solicitation might be a scam include:

- Refusal to give detailed information about the company's mission, costs, and how the donation will be used.
- Will not show proof that a contribution is tax deductible.
- High-pressure tactics to get you to donate immediately, without giving you time to think about it and do your research.
- Asking for donations in cash or a money wire.
- Offering to send a courier or overnight delivery service to collect the donation immediately.

PREVENTION TIPS

- Research the charity with The Better Business Bureau or Charity Navigator before making a donation or providing personal information.
- Never send cash donations.
- Remember that charity scams are not only a matter of money. In some cases, the scammer might attempt to seek personal identifying information through invasive forms or emailed solicitations.

SENIOR SCAMS

Scams that intentionally seek out and victimize seniors continue to be a nationwide problem. The elderly have long been targeted due to an assumed lack of knowledge about technology and ample access to financial resources. Scammers also consider the elderly to be less likely to ask for help or prosecute, making it a lower risk crime.

An elderly woman in her early 80s fell victim to one variation of the grandparent scam. In this case, scammers convinced her that a relative was arrested and was in dire need of help. She was prompted to put $12,000 on iTunes gift cards and then read the cards' serial numbers over the phone to the scammers. She was out $12,000 almost immediately after.

THREATS

- **Grandparent Scams**: In "grandparent scams," individuals will receive a call from a scammer pretending to be the victim's grandchild. The grandchild requests immediate assistance due to some sort of incident such as being put in jail or having a flight canceled. Their plea usually includes a request to not tell anyone (including parents) about their problem. The scam works well because it plays on the victim's emotions by making them feel distressed about their relatives. The twist during this particular time of year is that the grandchild wants to be "home for the holidays."

- **Utility Scams:** Scammers will often target the elderly with phone calls claiming that they are behind on payments and threaten to turn off power, heat or water. The fear that this instills in victims often causes them to hand over money quickly to avoid being left in the cold/heat or without water.

PREVENTION TIPS

- If a grandchild calls asking for assistance, ask them a wide array of questions including those that would be hard for the imposter to answer correctly.

- Slow the process down. Think twice before saying yes to a money transfer based on one call.

- Obtain as much information as you can, hang up and attempt to contact your relatives to confirm they are OK.

TRAVEL SCAMS

The holidays generally see an increase in consumer travel, and scammers are well aware. During the Holiday Season, long-distance travel can increase by as much as 54 percent, providing an opportunity for identity thieves.

THREATS

- **Phishing Emails with Fake Travel Deals:** There are an abundance of phishing emails promising unbelievable deals designed to steal your funds.
- **Fake Booking Websites:** These fake websites offer accommodations that do not exist as a ploy to capture your information and money.
- **ATM Skimming:** Skimming devices are rampant in areas where travelers are common. These devices are inserted into ATMs and capture the user's card information and PIN which is then used to drain the user's bank account.
- **Hotel Wi-Fi:** Information entered onto websites while using unsecured hotel Wi-Fi can be seen and captured by cybercriminals. Hotels are often a target because of the large number of people using the unsecured network.

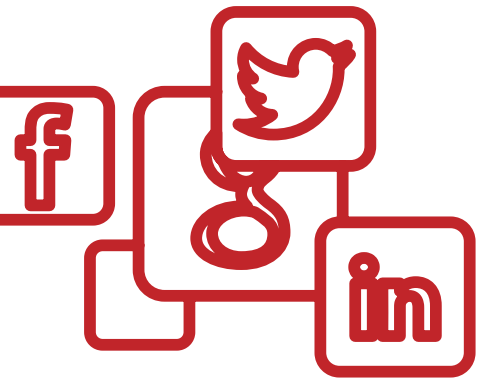
PREVENTION TIPS

- Be sure to use only legitimate, trustworthy travel booking sites before entering any personal details. Avoid too-good-to-be-true offers and flashy sidebar ads.
- Limit your use of public Wi-Fi as much as possible. Never access your financial account or any other sites that require a password when using it.
- Be cautious when using ATMs. Inspect the machine carefully before inserting your card. Fraudsters can attach card skimmers to the slot that capture your information when you insert it; very often, these look like they are part of the machine. Also, always shield the keypad when entering your PIN – scammers can also set up hidden video recorders. The safest ATMs to use are attached to banks in well-lit areas.

ONLINE & SOCIAL MEDIA SCAMS

Social media use by American consumers has seen year-over-year increases since 2008, and 2017 is already at the recorded highest point with an estimated 81 percent of consumers using social media. Due to the high volume of people worldwide who use it on a daily basis, there is little doubt as to why scammers took to these platforms.

A woman received a Facebook friend request from a stranger. They couldn't meet in person because the man claimed his contract with his employer wouldn't let him leave the state. Regardless, they quickly started emailing and talking on the phone for hours. Two months into their courtship, the man asked her to pay his taxes and she obliged with a wire transfer. She received another message with a request to pay an anti-terrorist fee. At that moment, she realized she was being scammed. Although she attempted to stop payment, the money, totaling $24,250 was already gone.



THREATS

- **Online Romance Scams:** The holidays are a time where some might feel lonelier and are more apt to fall for a romance scam, also called a "sweetheart scam." One of the ways this scams works is that a person receives a message or a friend request through a social media platform. Their courtship typically lasts a few weeks to a few months – just long enough that trust is built to start angling for money. The requests for money might be related to travel to come see you, a series of costly problems, or it could be related to paying for holiday gifts.

- **Social Media Scams:** During the holidays, scammers will often target you using social media with scams that are customized for the holidays. These scams include posts with links to fake surveys, giveaways, or fake coupons and discounts. Given the platform it's taking place on, all it takes is one person to share it or re-post it for the scam to easily go viral. Other social media scams include postings about bogus gift card offers and fake news stories that lure victims to websites that distribute malware.

PREVENTION TIPS

- Think before you click on any link and also before you re-share a post on social media.
- Avoid oversharing to prevent criminals from learning too much about you unnecessarily.
- Create strong passwords and refrain from re-using them.
- Do not accept friend requests from unknown parties.
- Never send money to someone you don't know.

CONCLUSION

With the number of scams likely to increase each year, especially during the holiday season, it's important to be extra vigilant in protecting your personal information and your finances. There is a multitude of free resources offered by organizations like the Identity Theft Resource Center to assist you. Another option is to work with a company that provides comprehensive identity protection that includes educational resources, online data protection, credit and identity theft monitoring alerts for proactive protection against fraudulent use of personal information. Additionally, these companies can provide full-service resolution shold you become a victim.

Becoming a victim of a scam at any time of the year is an awful experience. However, having to deal with the repercussions of a scam during the holidays is even harder. The extra layer of hectic schedules and financial burdens can make this a nightmarish experience at a time of year that should be enjoyed with friends and family. However, being armed with the above information and resources should help protect consumers against scams and increase the odds of a wonderful holiday season.

SUMMARY REFERENCES

Better Business Bureau. (2017, February 27). BBB Tip: Fake Check Scams. Retrieved from https://www.bbb.org/fakecheckscam/

Brenoff, A. (2016, December 9). Holiday Scams That Target The Elderly Just Came Roaring Back. Retrieved from https://www.huffingtonpost.com/entry/holiday-scams-that-target-the-elderly-just-came-roaring-back_us_584aef83e4b0bd9c3dfc8fd5

Bureau of Transportation Statistics. (n.d.). U.S. Holiday Travel. Retrieved from https://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/america_on_the_go/us_holiday_travel/html/entire.html

Ell, K. (2017, June 20). FBI says Internet romance scams on the rise. Here's what you need to know. Retrieved from https://www.usatoday.com/story/money/2017/07/20/fbi-says-internet-romance-scams-rise/485311001/

Federal Trade Commission (FTC). (June 2012). Before Giving to a Charity. Retrieved from https://www.consumer.ftc.gov/articles/0074-giving-charity#Signs

Fredman, C. (2015, December 16). Avoid Online Scams While Holiday Shopping. Retrieved from https://www.consumerreports.org/consumer-protection/avoid-online-scams-while-holiday-shopping/

Generali Global Assistance. (2016, July 11). Tips for Keeping Traveling Employees Safe from Identity Theft. Retrieved from http://irisidentityprotection.com/articles/tips-keeping-traveling-employees-safe-identity-theft/

Generali Global Assistance. (2016, November 9). Giving Customers and Employees the Gift of Identity Protection during the Holidays. Retrieved from http://irisidentityprotection.com/articles/giving-customers-employees-gift-identity-protection-holidays/

Generali Global Assistance. (2017, November 2). Three-Quarters of Americans Concerned About Identity Theft During Holiday Shopping Season. Retrieved from http://irisidentityprotection.com/news/three-quarters-americans-concerned-identity-theft-holiday-shopping-season/

Identity Theft Resource Center (ITRC). (2017, December 6). Data Breach Reports. Retrieved from http://www.idtheftcenter.org/images/breach/2017Breaches/DataBreachReport_2017.pdf

Identity Theft Resource Center (ITRC). (n.d.). Fake Wifi Hotspots. Retrieved from http://www.idtheftcenter.org/Current-Scam-Alerts/fake-wifi-hotspots

Identity Theft Resource Center (ITRC). (n.d.). New Grandparent Scam. Retrieved from http://www.idtheftcenter.org/Current-Scam-Alerts/new-grandparent-scam

Identity Theft Resource Center (ITRC). (n.d.). Your Identity Theft Holiday Checklist. Retrieved from http://www.idtheftcenter.org/Identity-Theft/your-identity-theft-holiday-checklist-2

Identity Theft Resource Center (ITRC). The Harm in Hoaxes on Social Media. Retrieved from http://www.idtheftcenter.org/Cybersecurity/the-harm-in-hoaxes-on-social-media

Iliopoulos, M. (2017, October 17). BBB: Employment scams spike amid holiday hiring frenzy. Retrieved from http://www.thedenverchannel.com/news/local-news/bbb-employment-scams-spike-amid-holiday-hiring-frenzy

Kirchheimer, S. (2016, November 18). Job Scams: Tip-Offs to Rip-Offs. Retrieved from http://blog.aarp.org/2016/11/18/job-scams-tip-offs-to-rip-offs/

Lipka, M. (2011, December 21). Romance scams on the rise over the holidays: report. Retrieved from http://nationalpost.com/news/canada/romance-scams-on-the-rise-over-the-holidays

Mayer, S. (2017, September 24). Beware of seasonal employment scams. Retrieved from http://www.argusobserver.com/business/beware-of-seasonal-employment-scams/article_73d14dc0-a0be-11e7-9909-4f5ca2d0eec2.html

McCoy, K. (2017, May 23). Target to pay $18.5M for 2013 data breach that affected 41 million consumers. Retrieved from https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

Morad, R. (2016, November 30). 5 Naughty Scams To Watch Out For This Holiday Season. Retrieved from https://www.forbes.com/sites/reneemorad/2016/11/30/5-naughty-scams-to-watch-out-for-this-holiday-season/#69c60fa63b70

National Council on Aging (NCOA). (n.d.). Top 10 Financial Scams Targeting Seniors. Retrieved from https://www.ncoa.org/economic-security/money-management/scams-security/top-10-scams-targeting-seniors/

Shadel, D and Park, K and Newman A. (November 2015). Beware the Grinch: American Consumers at Risk of Being Scammed During the Holidays. Retrieved from https://www.aarp.org/research/topics/economics/info-2015/national-holiday-scam-survey.html

Statista. (n.d.). Percentage of U.S. population with a social media profile from 2008 to 2017. Retrieved from https://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/

Steinberg, J. (2016, August 10). 8 Ways to Protect Yourself From Scams on Social Media. Retrieved from https://www.inc.com/joseph-steinberg/8-ways-to-avoid-scams-when-using-social-media.html

Steinberg, J. (2016, December 13). Beware These 6 Holiday Season Social Media Scams. Retrieved from https://www.inc.com/joseph-steinberg/beware-these-6-holiday-season-social-media-scams.html

Steinberg, J. (2016, June 6). How to Be Better at Social Media Than Mark Zuckerberg. Retrieved from https://www.inc.com/joseph-steinberg/how-to-be-better-at-social-media-than-mark-zuckerberg.html

Stolley, R. (January/February 2017). How to Beat the Grandparent Scam. Retrieved from https://www.aarp.org/money/scams-fraud/info-2016/how-to-beat-grandparent-scam.html

Generali Global Assistance (GGA), proudly owned by Europ Assitsance Holding, a division of the multinational Generali Group, has been busy protecting clients and their customers for over 30 years–via co-branded services and behind the scenes as a client-branded provider. GGA was one of the first companies to provide identity theft resolution services in the United States. They are the identity protection engine behind some of the biggest names in the Fortune 500, and today are a leading provider, proudly protecting millions of lives from the growing threat of identity theft. Their comprehensive identity protection is a powerful combination of credit monitoring and alerts, advanced identity monitoring technology, online data protectoin tools, and award-winning resolution.

For more information about preventing identity theft for your employees, customers, or members, contact Generali Global Assistance Identity Protection Services at

GeneraliGlobalAssistance-IDP.com

GENERALI
GLOBAL ASSISTANCE

Founded in 1999, the Identity Theft Resource Center® (ITRC) is a nationally recognized non-profit organization established to support victims of identity theft in resolving their cases, and to broaden public education and awareness in the understanding of identity theft, data breaches, cybersecurity, scams/fraud, and privacy issues.

The ITRC provides no cost victim assistance and consumer education through its call center, website, social media channels, live chat feature and ID Theft Help Mobile App.

www.idtheftcenter.org

ITRC | IDENTITY THEFT RESOURCE CENTER