Information Technology Division Bulletin

vol. 19 no. 4 | December 2022

Message from the CIO

As the fall semester draws to a close and the holiday season is upon us, we provide information for securing your personal data from prying eyes. For those traveling, we provide some tips to help protect institutional and personal information. To help ensure a healthy holiday, we include ways to sanitize your phones and other devices. Finally, be sure to read about the 12 scams of Christmas to ensure you do not fall prey to holiday scammers and criminals. We encourage you to stay vigilant and protect your personal and TTU's information. From our families to yours, Season's Greetings – and a safe holiday season. Have a restful winter break. Go Tech!

—Sam Segran, Vice President for IT and Chief Information Officer

Protecting your Data from the Crowd: How to Prevent "Shoulder Surfing"

The holiday season brings people together, and that means crowds. Whether you are at holiday gatherings, venturing out among holiday shoppers, or simply standing in lines at airports, protecting your personal data from scammers requires vigilance.

Shoulder surfing is the attempted theft of your data from thieves who spy over your shoulder as you use a smartphone, laptop, or ATM in busy public spaces. These shoulder surfers blend into the crowd and maneuver to observe your mobile device screen and keyboard to obtain sensitive information. Shoulder surfing has even evolved where direct observation is often unnecessary, replaced with scammers using binoculars or hidden video cameras.

Tips to Protect your Data from Shoulder Surfing:

- When possible, avoid entering sensitive data on your laptop, tablet, or smartphone in a public place.
- Use two-factor authentication; this extra layer of protection makes it more difficult for scammers to steal your data, as one compromised action alone will not be enough to breach your security.
- When using devices in a public space, utilize your body and surroundings to shield your data physically. Move away from the center of the crowd and avoid open spaces when using your devices and cover ATM keyboards with your off-hand as you input your PIN or password.
- Apply a privacy filter to your laptop or smartphone. Privacy filters are polarized translucent sheets that, when placed over the screen, obscure it from onlookers attempting to view the screen.
- Consider using a password manager. Password managers store your commonly used passwords preventing the need to re-enter them in public and potentially exposing your data to prying eyes.

How to Sanitize Your Devices

Hand washing has long been adopted as a necessary procedure, but what about sanitizing your devices? Have you committed to keeping those clean as well? Taking extra precautions to avoid contamination is more important now than ever before.

In the wake of COVID-19, Consumer Reports created a video on how to sanitize electronic devices. Additionally, Apple released cleaning instructions for all Apple products. The TTU IT Division encourages you to follow their guidelines:

- Clean your device immediately if it comes into contact with any damage-causing material (liquid, oils, sand, etc.);
- Do not spray cleaners directly onto the device;
- Unplug all external power sources, devices, and cables when cleaning the product;
- You may use 70% isopropyl alcohol, disinfecting wipes, or a similar product without bleach;
- Do not get moisture into any openings;
- Do not use aerosol sprays, bleaches, ammonia, or abrasives;
- Use only a soft, lint-free cloth. Do not use paper towels, tissues, or similar because they are abrasive; and
- Avoid excessive wiping, which might cause damage.

The Naughty List: 12 Scams of Christmas

Reprinted in its entirety with permission from BBB: The naughty list - BBB's 12 scams of Christmas, Sept. 2022, https://www.bbb.org/article/news-releases/23497-the-naughty-list-bbbs-12-scams-of-christmas.

With 2022 quickly winding down, **Better Business Bureau has compiled our naughty list of the top 12 scams of Christmas.** When shopping or donating this holiday season, watch out for schemes trying to swipe your cash or steal your personal information.

You can avoid most of the scams on this list by taking a few simple precautions. Always exercise caution with social media ads promoting discounted items, holiday events, job opportunities, and donation requests, as well as direct messages from strangers. If you are asked to make a payment or donation by wire transfer, through a third party, or by prepaid debit or gift card, treat it as a red flag.

Be mindful of these scams that could cut into your holiday cheer

1. **Misleading social media ads**: As you scroll through your social media feed, you often see products advertised. Always research before you buy. BBB Scam Tracker receives daily reports of people paying for items that they never receive, getting charged monthly for a free trial they never signed up for, or receiving an item that is counterfeit or much different from the one advertised. The 2022 BBB Online Scams Report found that online purchase scams were the most common cons reported to Scam Tracker. Before ordering, check out the business profile on BBB.org and read the reviews. Read more about misleading ads, free trial offers, and counterfeit goods.

2. **Social media gift exchanges**: Each holiday season this scheme pops back up, and this year is no different. A newer version of this scam revolves around exchanging bottles of wine; another suggests purchasing $10 gifts online. Another twist asks you to submit your email into a list where participants get to pick a name and send money to strangers to "pay it forward." There is even a twist about "Secret Santa Dog" where you buy a $10 gift for your "secret dog."

In all of these versions, participants unwittingly share their personal information, along with those of their family members and friends, and are further tricked into buying and shipping gifts or money to unknown individuals. And-- it's an illegal pyramid scheme. Read more about the social media gift exchange.

3. **Holiday apps**: Apple's App Store and Google Play list dozens of holiday-themed apps where children can video chat live with Santa, light the menorah, watch Santa feed live reindeer, track his sleigh on Christmas Eve, or relay their holiday wish lists. Review privacy policies to see what information will be collected. Be wary of free apps, as they can sometimes contain more advertising than apps that require a nominal fee. Free apps can also contain malware. Read more about holiday apps.

4. **Alerts about compromised accounts**: BBB has been receiving reports on Scam Tracker about a con claiming your Amazon, Paypal, Netflix or bank account has been compromised. Victims receive an email, call, or text message which explains that there has been suspicious activity on one of their accounts, and it further urges them to take immediate action to prevent the account from being compromised. Be extra cautious about unsolicited calls, emails, and texts. Read more about compromised account scams.

5. **Free gift cards**: Nothing brings good cheer like the word "FREE." Scammers have been known to take advantage of this weakness by sending bulk phishing emails requesting personal information to receive free gift cards. In some of these emails, scammers impersonate legitimate companies and promise gift cards to reward their loyal customers. They may also use pop-up ads or send text messages with links saying you were randomly selected as the winner for a prize.

If you have received an unsolicited email with gift card offers, do not open it. Instead, mark it as spam or junk. However, if you opened the email, do not click on any links. Read more about gift card scams.

6. **Temporary holiday jobs**: Retailers typically hire seasonal workers to help meet the demands of holiday shoppers. Shippers and delivery services are top holiday employers this year because of the increase in online orders and the need to get most of these packages delivered before Christmas. These jobs are a great way to make extra money, sometimes with the possibility of turning into a long-term employment opportunity. However, job seekers need to be wary of employment scams aimed at stealing money and personal information from job applicants. Keep an eye out for opportunities that seem too good to be true. Read more about holiday job scams.

7. **Look-alike websites**: The holiday season brings endless emails offering deals, sales, and bargains. Be wary of emails with links enclosed. Some may lead to look-alike websites created by scammers to trick people into downloading malware, making dead-end purchases, and sharing private information. If you are uncertain about the email, do not click any of the links. Instead, hover over them to see where they reroute. Read more on look-alike websites.

8. **Fake charities**: The last few weeks of the year is a busy time for charitable donations. Donors are advised to look out for fraudulent charities and scammers pretending to be individuals in need. Avoid impromptu donation decisions to unfamiliar organizations. Responsible organizations will welcome a gift tomorrow as much as they do today. Verify a charity at BBB's Give.org or on the Canada Revenue Agency website. Where possible, donate to the charity through their website and use a credit card. Read more about fake charities.

9. **Fake shipping notifications**: More consumers are making purchases online, and there is also an increase in the number of notifications about shipping details from retailers and carriers. Scammers are using this new surge to send phishing emails with links enclosed that may allow unwanted access to your private information or download malware onto your device. They may also try to trick people into paying new shipping fees. Read more about delivery and package scams.

10. **Pop-up holiday virtual events**: Many local in-person events such as pop-up holiday markets or craft fairs, have moved online. Scammers are creating fake event pages, social media posts, and emails, charging admission for what used to be a free event. The goal is to steal credit card information. Confirm with the organizer of the event if there is an admission fee. In cases where there is a charge, use a credit card. If the event is free, watch for scammers trying to claim otherwise. Read more about pop-up holiday shops.

11. **Top holiday wishlist items**: Low priced luxury goods, jewelry, designer clothing, and electronics are almost always cheap counterfeits and knockoffs. The same applies for popular toys. This year, Squishmallows, Magic Mixies Magical Misting Crystal Ball, Snap Circuits, Breyer Horses Unicorn Magic Wood Stable, and National Geographic Break Open Geodes are some of the items in high demand. Be very cautious when considering purchasing these popular toys from resellers on Facebook Marketplace and other platforms. Read more about holiday hot toy scams.

12. **Puppy scams**: Many families may be considering adding a furry friend to their household this year. However, be on the lookout for scams. Many would-be pet owners turn to the internet to find their future cat or dog, but experts say a shocking 80% of sponsored pet advertisements may be fake. Be sure to see the pet in person before making a purchase. Read more on pet scams.

For general information on how to avoid scams, visit BBB.org/AvoidScams. For more advice, read BBB's tips on online shopping. If you've spotted an online scam, report it to BBB ScamTracker. ***Read more BBB Holiday Tips at BBB.org/holiday.***

Holiday Travel

Travelers may face an increased risk of identity theft if they carry debit/credit cards, passports, and other official forms of personal identification. As a result, vacationers are regularly targeted by criminals, who are just as likely to go after your personal information as they are your laptop or smartphone. To help protect your identity and information, the TTU IT Division recommends the following best practices while traveling:

- **Carry a limited number of credit cards to limit your exposure to theft**. We recommend that you notify those credit card companies about your travel and make sure you know how to contact them in the event your credit cards are stolen or lost;
- **Take advantage of the hotel safe** rather than leaving personal items in your hotel room;
- **If you make travel arrangements using a mobile device, avoid storing transaction information**, such as login information, credit card number, or billing address. Remember that saved information could be stolen along with your phone;
- **Protect your computers and mobile devices** (including phones) with passwords;
- **Public wireless connections are not secure**, so avoid using them for secure transactions, such as transactions requiring a login; and
- **Stay alert! It is easy to let your guard down while relaxing on vacation**, but it's essential to be aware of your surroundings and the people around you.