

OCS, IT Security Watch Holidays 2019



Have a safe and secure Holiday



Cyber Tips for Social Media

Tis the season for sharing, but when it comes to social networking, some people may share too much about their whereabouts and the gifts they'll give.

1. Change Account Settings – The simplest and most effective way to stay aloof online is to update your account settings within all of your social media apps, as well as on all of your electronic devices that you use to post.

- Turn off your location services (geotagging) for camera and photos.
- Change your privacy settings within each social media app to limit your posts' exposure.
- Edit what your friends/followers are allowed to post on your timeline or tag you in their own posts. Postpone accepting friend requests until after the holidays, unless you are expecting one from a family member or close friend.

2. Limit Posting – While we encourage you to unplug through the holidays, you may still find yourself surfing news feeds and wanting to post occasionally about your own holiday cheer.

- Definitely avoid posting your travel plans and photos telling the world you are not home.
- If you're staying in town, avoid posting about your holiday events/festival plans. It only takes a few minutes to burglarize home.
- Don't check-in! You might be really excited about attending a big event, but posting it to the public can wait until you are home.

Just Unplug.
The safest way to protect yourself from potential holiday cyber crime, is to simply unplug! Just sit back and enjoy a truly wireless holiday break.

Home Security for the Holidays

- Be extra cautious about locking doors and windows when you leave the house, even for a few minutes.
- When leaving home for an extended time, have a neighbor or family member watch your house and pick up your newspapers, mail (or stop at post office) and even take trash cans in/out at the curb.
- Indoor and outdoor lights should be on an automatic timer.
- Leave a radio or television on so the house looks and sounds occupied.
- Large displays of holiday gifts should not be visible through the windows and doors of your home.
- When setting up a Christmas tree or other holiday display, make sure doors and passageways are clear inside your home.
- Be sure your Christmas tree is mounted on a sturdy base so children, elderly persons or family pets cannot pull it over on themselves.
- If you use lights on your Christmas tree ensure the wiring is not damaged or frayed. Frayed or damaged wiring can cause a fire.
- Place your Christmas tree in water or wet sand to keep it green.



Picture the scene: The presents have been unwrapped, the gizmos and gadgets are ready to be played with, but the living room looks like the aftermath of a Christmas war. You're tempted to stack the boxes and packaging at the curb just to claim your living room back. Stop! You don't want to advertise those awesome gifts to shady characters circling the block looking for their next score.



OR
Christmas tip: put your Christmas trash in your neighbors bin so they get robbed instead of you.



12 SCAMS of Christmas

Look-Alike Websites
When stores sell out, you may find the items online on different websites than the official retailer's. Remember, it's easy to mimic a real website. Some sellers will take your money and run, leaving you without the gift or money to buy it elsewhere.

Fake Shipping Notifications
These can have attachments or links to sites that will download malware on your computer to steal your identity and your passwords. Don't be fooled by a holiday phishing scam.

Social Media Gift Exchange
Purchasing one gift and receiving 36 sounds like a great deal, but this seasonal scam is actually a pyramid scheme, which is illegal.

Phony Charities
Everyone is in a generous mood during the holidays, so scammers take advantage of that with fake charity solicitations in email, on social media sites, and even by text. Check out charities at give.org before donating.

Grandparent Scams
Seniors should be cautious if they get a call from a grandchild claiming to be in an accident, arrested or hospitalized while traveling in another country. Never send money unless you confirm with another family member that it's true.

Letters From Santa
Several trusted companies offer charming and personalized letters from Santa, but scammers mimic them to get personal information from unsuspecting parents. Check with bbb.org to find out which ones are legitimate.

Temporary Holiday Jobs
Retailers and delivery services need extra help at the holidays, but beware of solicitations that require you to share personal information online or pay for a job lead. Apply in person or go to retailers' main website to find out who is hiring.

Unusual Forms of Payments
Be wary of anyone who asks you to pay for holiday purchases using prepaid debit cards, gift cards, wire transfers, third parties, etc. These payments cannot be traced and cannot be undone.

Free Gift Cards
Pop-up ads or email offering free gift cards are often just a ploy to get your personal information that can later be used for identity theft.

Travel Scams
With busy holiday travel, bargains may be tempting. Be cautious when booking through online ads, never wire money to someone you don't know and ask for references.

E-Cards
Electronic cards can be great fun, but be careful. Two red flags to watch out for are: the sender's name is not apparent; you are required to share additional information to get the card.

Puppy Scams
Be very careful buying pets online, especially during the holidays. You may get a puppy mill pooch with problems, or you may get nothing at all because it was a scam.

For more information on these scams, go to bbb.org

Online Shopping Tips

Do not use public Wi-Fi for any shopping activity.

Public Wi-Fi networks can be very dangerous. To help stay secure, you should always be on the lookout for the lock symbol on your webpage. Never bank from public Wi-Fi.

One-time use credit card numbers.

This one-time number is associated with your account and can be used in place of your credit card number. Check with your credit card company or bank to see if they have this option available.

Check out as a guest.

By checking out as a guest, you prevent the online retailer from storing your personal account and financial information. This minimizes the amount of information that could be lost if the retailer is compromised.

