HOLIDAY MALWARE

DEPARTMENT OF AVIATION INFORMATION SECURITY UPDATE

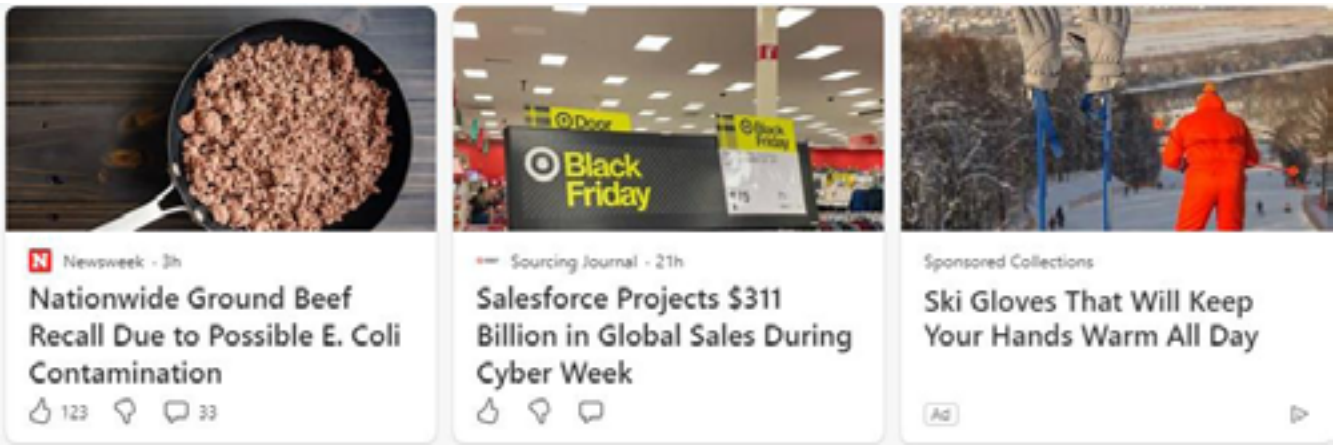
Happy December PHL/PNE Team!

As we head into the holidays and end of the year festivities it's important to remember that this month is "the most wonderful time of the year" for more than just us. Malware/Ransomware gangs, threat actors, and novice hackers use this time of joy, distractions, and PTO to launch some of their most vicious attacks. So, this month the Infosec Team would like to provide some helpful tips to avoid an unwanted present under your tree.In aviation, data privacy concerns range from the personal details passengers provide when booking a flight to the biometric data used in modern boarding processes. Companies must stay transparent about how this information is used and give the passengers control over their data. Passengers must know their rights and the privacy policies of the airlines and airports they engage with to ensure their data is managed responsibly.

Malware Malware Everywhere (and there's much more than you think)

As a reminder, Malware is short for "Malicious Software" and it covers wide range of tools and applications designed to invade your privacy, compromise your accounts, and steal your information. Just like anything else infectious (and trust us, malware will get everywhere if you let it) there are some things that you can do to prevent yourself and those around you from being the latest targets. Here's what the Infosec Team recommends:

1. **Be cautious about news media links**
   Not all news is good news, and that's especially true when it comes to the links to news sites that appear on our browser homepages. These links and their attention-grabbing headlines are designed to pull your focus and make you act before you have a chance to think. This is exactly what attackers want you to do, but please don't take the bait! In November, the Infosec team discovered that Russia-based attackers have been exploiting these links to redirect users to malicious sites. These sites appear legitimate, and the links are indistinguishable from a secure site at first glance. We recommend visiting your preferred news media outlet's website directly to avoid this issue.



These links appear legitimate, but they could be hiding malware!

2. **Look out for strange deals/offers via email or text**
   By now (and especially after October's security awareness training) you are probably an expert on spotting phishing attempts and cybersecurity threats, but the end of the year festivities tend to make even the best of us drop our guard, and that is when attackers do their worst work. Be on the lookout for emails that sound too good to be true. Text alerts that appear to be from FedEx or UPS, Special offers, limited time holiday deals, and random gift card rewards are just a few of the favorite tricks and traps that attackers use to make sure you get malware instead of that new car that you've been dreaming of.

3. **Practice good cyber hygiene**
   There's no time better than the end of the year to take a look at your accounts and make sure everything is as secure as possible. Every year hundreds of thousands of passwords and account credentials end up on the Dark Web for attackers to purchase and exploit, and there's a good chance that old password that you haven't updated in years is among them. Attackers can use these credentials to sign into your accounts, send phishing emails to your friends, family, and colleagues, and truly steal your Christmas. Take a moment to update your old or reused passwords and make sure all your data is stored in a secure place.

Don't let this guy steal your Christmas!

Following these tips will help keep your data secure as your attention drifts away from thoughts of work and on towards your loved ones and the upcoming year. This is a special time of year for all of us and as long as we don't give the attackers a chance to ruin it, we can help to keep it that way.

Remember: when it doubt, don't click. Report it quick.

Happy Holidays and Stay Frosty,
The Infosec Team