Cyber Safety during the holidays

Office of Information Technology
Division of Information Security
DECEMBER 2021

As the

end of the year approaches, more people are taking leave, trying to find the best online deals, and using social media to connect with family and friends. While these activities can help us recharge and get closer to those we care about the most, they also provide opportunities for malicious actors to fool us into handing over information, usually for a financial reward. It only takes a moment to fall victim to fraud, but takes much longer to recover from the mistake. Let's take a look at how this time of year creates opportunities for bad actors and what you can do to avoid them.

When taking leave, set an out of office email so that people know when you'll return and who they can contact in your absence. Take care to provide only the most basic information, especially for replies to emails from outside the organization. Best practice is not to include your out of office location or a specific contact name, instead directing them to use a shared inbox. By providing the dates of your leave, the destination, and a trusted agency contact in your out of office reply, a malicious person has more information reach out to that person and pretend to be you. They will rely on the familiarity of the relationship to fool your contact into making a decision that can have significant negative financial and reputational consequences, like the loss of funds or unauthorized release of information.

TIP

If you ever get an email or phone call asking you to release money or provide information, use a different method to contact the person making the request. Then verify their identity, and the validity of the request.

Knowing that many people are looking for gifts online, bad actors will send fraudulent, but seemingly authentic, shipping notices via email or text message. Most commonly, these notices will include a link or attachment, asking you to click the link to enter your credentials or download the attachment. Entering credentials allows the attacker to capture and use them for their own purposes, while the download contains infectious malicious code that will execute its program.

TIP

When you get a shipping notification, check the shipper's Web site yourself to determine whether the notification is real.

In our social media posts and interactions, sharing can be caring, but we should also share with care. Check settings on all of your social media accounts to ensure you are sharing only what you want, with whom you want. Settings include connections, status visibility, updates, locations, and photographs. When possible, make sure all of your social media accounts require two-factor authentication for access, so that even if your password is compromised, it's harder to access the account. Only accept requests to connect from people you know and trust. Posting pictures of gift card numbers gives scammers all the information they need to go to the merchant's online store and spend those funds.

TIP

While these are great tips for the holiday season, you can, and should, use them all year to keep your information safe. Protecting your information goes a long way toward protecting yourself, as well as everyone and everything you hold near and dear. For questions, please contact cybersecurity@ihs.gov.