ITS Communications

Algonquin College
Cybersecurity
Awareness Month
2024

Phishing During the Holidays

Around the holidays, inboxes everywhere are flooded with shipping updates, order confirmations, and eCards from family and friends. Attackers take advantage of the deluge of emails by sending creative phishing emails designed to catch targets off guard. From fake charity websites to malicious eCards, cyber attacks spike during the holiday season.

What to Look Out For

Shipping Updates

Fake shipping notifications increase each year around the holidays. With so many online orders being shipped, people may be more susceptible to clicking a link about a status update or a failed delivery. Even if the message looks valid, go to the site directly and enter the tracking number yourself. Call a shipping company for assistance using the contact information on their site.

Fake Order Confirmations

Attackers also take advantage of the increase in year-end online shopping from the most popular shopping days of the year—Black Friday and Cyber Monday. During this hectic time, you may be more likely to click an order confirmation link from your favorite company without questioning it. Keep track of your orders so you know what emails to expect.

Holiday eCards

Another popular lure that attackers use is sending fake eCards with malicious files attached. Although a cute eCard may look innocent, never click a link from an unknown source.

Charity Phishing Scams

Phishers often impersonate charities and send emails asking for year-end donations. Before entering personal information and making a donation, ensure that the site is legitimate and you recognize the domain. Also, ensure the URL shows “https://”, indicating that the connection is secure.

Unsolicited Offers and Deals

Around the holidays, inboxes are overflowing with messages about stunning deals and promotions. Attackers often target employees with end-of-year giveaways and contests. Don't click on any email offers or pop-up ads. Instead, verify that the offer is legitimate by going to the retailer's site and shopping there directly. Remember: if it seems too good to be true, it probably is.

Quick Tips

Think twice. Read emails thoroughly and be wary of offers that seem too good to be true.

- **Bookmark shopping sites.** Avoid using search engines to find deals. Using trusted shopping sites can help reduce the chance of landing on a malicious site.
- **Look at the domain name.** Some attackers modify domains to catch targets off guard. For example, if the correct domain was www.example.com, the phishers may register “examp1e.com” or “example.co”.
- **Always verify.** Verify that the email is from the real sender before engaging. Call or email the sender to confirm it is legitimate.

Remember that legitimate organizations will never ask for your password or other sensitive information via email; if you spot suspicious activity, make sure to report it using the Report Phishing Button or to spamorscam@algonquincollege.com

Did you know?
You can safely check where a link goes without clicking:

- Desktop (OSx and Windows): Hover your cursor over the link to view the URL.
- Mobile Devices (Android, iOS, Windows): Touch and hold the link until a pop-up menu appears.