WISCONSIN ELECTIONS COMMISSION

212 EAST WASHINGTON AVENUE, 3RD FLOOR
POST OFFICE BOX 7984
MADISON, WI 53707-7984
(608) 261-2028
ELECTIONS@WI.GOV
ELECTIONS.WI.GOV

INTERIM ADMINISTRATOR MEAGAN WOLFE

MEMORANDUM

TO: Wisconsin Municipal Clerks
City of Milwaukee Election Commission
Wisconsin County Clerks
Milwaukee County Election Commission

FROM: Meagan Wolfe, Interim Administrator
Tony Bridges, Election Security Lead

DATE: November 21, 2108

SUBJECT: Stay Safe Online During the Holidays

After the General Election earlier this month, everyone is looking forward to the holidays. However, cyber threats don't take breaks, and the holidays are prime targets for criminals.

Specifically, the Wisconsin Elections Commission has been made aware of a current phishing campaign directed at government employees. This campaign uses emails that appear to be sent from official government sites and have messages about Thanksgiving cards. However, an attached Word document carries malware. WEC staff would like to remind you to be cautious with emails and to verify the source of unexpected email attachments.

More generally, the WEC urges everyone to be mindful of holiday tricksters. Be on the lookout for these common scams listed by the Better Business Bureau:

Be cautious shopping online -- Because many retailers now have chip card readers, fraud at bricks-and-mortar stores is down, so scammers have shifted their efforts online. Use a credit (not debit) card online and only shop on secure websites. Look for "https" in the address (the "s" is for "secure") and for a lock symbol.

Watch out for look-alike websites – When shopping online, make sure to use only legitimate websites. Watch out for URLs that use the names of well-known brands along with extra words.

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.

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.

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.

Emergency scam – Be cautious if you get a call from a family member or friend 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.

Phony charities – Everyone is in a generous mood at 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.

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 websites to find out who is hiring.

Unusual forms of payment – 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.

Social media gift exchange – It sounds like a great deal: buy one gift and get 36 in return. But it's just a variation on a pyramid scheme and it's illegal.

Afraid you're a victim? – If you believe you are a victim of a scam or malware campaign, the US Computer Emergency Readiness Team in the Department of Homeland Security suggests taking the following actions:

- Contact your financial institution immediately, and close any accounts that may have been compromised. Watch for any unexplainable charges to your account. See Preventing and Responding to Identity Theft for more information.

- Immediately change any passwords you might have revealed. Avoid reusing passwords. See Choosing and Protecting Passwords for more information.

- Report the attack to the police, and file reports with the Federal Trade Commission and the FBI's Internet Crime Complaint Center.

Additionally, if you believe any of your work computers or devices have been compromised, immediately contact your IT department and the Wisconsin Elections Commission's Help Desk, 608-261-2028.