# News Release

**WI HOMELAND SECURITY ADVISORY COUNCIL**

Joint Force Headquarters ▪ 2400 Wright Street ▪ Madison, WI ▪ 53704

October 9, 2017


Contact: Wisconsin Department of Military Affairs

For more information contact:

| | |
|---|---|
| Tod Pritchard | Lori Getter |
| Office (608) 242-3324 | (608) 242-3239 |
| Cell (608) 219-4008 | (608) 516-0293 |


## WISCONSIN DEPARTMENT OF MILITARY AFFAIRS UPDATE: Cybersecurity in the workplace is everyone's business

Wisconsin Department of Military Affairs

MADISON, Wis. — Cyber criminals are sneaky — they are constantly coming up with new ways to get what they want. They like to target employees inside businesses and other organizations.

"Cyber attackers prey on the least prepared or least aware people and the effects are devastating," said Maj. Gen. Don Dunbar, Wisconsin's adjutant general and Homeland Security Advisor. "Cyber criminals develop new tactics that cause harm every day. It is incumbent upon everyone to be prepared, understand the threat, and take consistent action to protect or networks and information."

The most costly cyber scam happening right now is called CEO Fraud, also known as Business Email Compromise (BEC). In these attacks, the bad guys pretend to be a CEO or other senior executive from your organization.

"As technology becomes more advanced, so do the tactics of criminals targeting individuals online with phony schemes," said Attorney General Brad Schimel. "Sometimes, criminals send emails to individuals at their workplaces that appear fake or fraudulent. Other times, criminals use websites and emails that appear perfectly legitimate, borrowing official seals, logos, letterhead, and even masked email addresses and websites. If the cyber criminals are looking for money, they may target staff in the accounts payable department. If they are looking for tax information, they may target human resources. We must all remain vigilant and exercise extreme caution, consulting with IT experts regularly for the latest updates, tips, and verifications."

Phishing scams are also very common. Attackers sends an email to millions of people with the goal of tricking them into doing something, for example, opening an infected attachment or visiting a malicious website.

Spear phishing is similar to phishing; however, instead of sending a generic email to millions of people, they send a custom email targeting a very small, select number of people. These spear phishing emails are extremely realistic looking and hard to detect. They often appear to come from someone you know or work with, such as a fellow employee or perhaps even your boss.

Here are three common scenarios:

Wire Transfer: A cyber criminal is after money. This means they research and learn who works in accounts payable or the team that handles your organization's finances. The criminals then craft and send an email pretending to be the targets' boss; the email tells them there is an emergency and money has to be transferred right away to a certain account.

Tax Fraud: Cyber criminals want to steal information about your coworkers so they can impersonate employees for tax fraud. They research your organization and determine who handles employee information, for example, someone in human resources. From there, the cyber criminals send fake emails pretending to be a senior executive or someone from legal, demanding certain documents be provided immediately.

Attorney Impersonation: Not all CEO Fraud attacks involve just email; other methods like the telephone can be used. In this scenario, criminals start by emailing you pretending to be a senior leader, advising you that an attorney will call about an urgent matter. The criminal then calls you pretending to be the attorney. The criminal creates a tremendous sense of urgency as they talk about time-sensitive, confidential matters. This sense of urgency tricks you into acting right away.

So what can you do to protect yourself and your organization? Common sense is your best defense. If you receive a message from your boss or a colleague and it does not sound or feel right, it may be an attack. When in doubt, call the person at a trusted phone number or meet them in person (don't reply via email) and confirm if they sent the email.

These and many other topics will be discussed at Wisconsin's 5th Annual Governor's Cybersecurity Summit, Monday, Oct. 16 at the Gordon Event Center, UW-Madison. Learn more about the Summit and register online at http://cybersummit.wisconsin.gov.

This October, ReadyWisconsin will highlight efforts to keep everyone in Wisconsin safe from cybercrime. Visit http://readywisconsin.wi.gov for more information. You can also follow us on Twitter, Facebook, and Instagram.

- 30 -

**To see this content online, copy the following link and paste in your browser: http://dma.wi.gov/DMA/news/2017news/17130**

**Join us on Twitter at http://twitter.com/ReadyWisconsin, Facebook at http://www.facebook.com/ReadyWisconsin, and Instagram at www.instagram.com/readywisconsin**

**Current News Releases and Media Galleries**

**Facebook: Common sense is the first line of #cybersecurity defense against phishing attacks**

# News Release

**WI HOMELAND SECURITY ADVISORY COUNCIL**

Joint Force Headquarters ▪ 2400 Wright Street ▪ Madison, WI ▪ 53704

**Post: DMA, WEM, ReadyWI, Homeland Security**

**GovDelivery Audiences: 2017 WI Legislature, WI Media, 2017 Congress, Governor's Office, WEM EMS and Regions, Homeland Security, ReadyWI, WI EM News**

**Expiration Date: Third in 5-part series**