your energy partner®
OPPD
Omaha Public Power District

SHIELD
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
Information Protection Newsletter

CEO Fraud Attacks on the Rise in 2019

By Trustwave: Empowering End Users by Providing Knowledge and Defining Best Practices

Cyber-criminals are spoofing CEO and other Sr. Executives email accounts and requesting that employees buy gift cards or perform other transactions for him/her. We're all drowning in emails but let's admit one thing: We all perk up when we see a message from our CEO or the Director show up in our inbox.

Suddenly all the email noise reduces to a whisper, and all your focus shifts to this single message. Depending on your current level of paranoia, your mood may quickly turn to dread. You breathe a sigh of relief when you realize you're done nothing wrong and aren't being asked to work over the weekend. Instead, your boss just needs a quick favor, a simple funds transfer or an urgent request for a few 'reward gift cards' to give to a customer or employee.

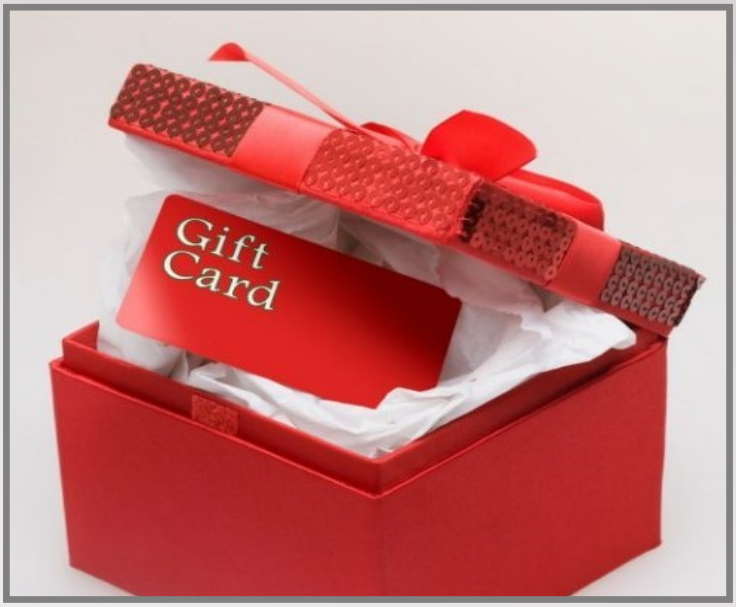
What do you do? The default, of course, is to comply with the boss' wishes. Love them or hate them, satisfying their work demands is generally a safe way to stay on their good side. But what if you weren't so quick to respond - or didn't at all?

The chances that such an email has been completely fabricated by an external adversary fixed on stealing from your company is rapidly growing. Business email compromise scams (BEC), which typically combine spear phishing, email spoofing, social engineering (and occasionally malware), have steadily grown into a prolific problem for businesses of all sizes, resulting in massive losses to the tune of several billion dollars.

These messages typically bypass the spam filter because they are not part of a mass-mailing campaign and are instead more targeted in nature, usually missing the typical junk mail traits. A recent survey by the Association of Financial Professionals, which polled treasury and finance professionals, found that 77 percent of organizations experienced attempted or actual BEC scams - commonly called CEO fraud - in 2017.

The attackers smartly make their email sound convincing, without delving into any deep conversation that would give them away as being an impostor.

One other caveat worth noting about these crafted emails is the quality. Normal spam messages contain easy-to-identify grammatical and spelling errors buy not so much for CEO fraud. These are targeted, one-on-one operations conducted



individually by con artists targeting specific companies (and specific individuals at those companies) and all they require is that the perpetrator be fluent in the victim's language.

The conversations start with small requests, and after trust is established, and have a valid email address, they will start their seemingly 'harmless' requests.

So what can you do to avoid these traps? Educate users to be on the lookout for these type of scams. Know how to identify them and what to do if you believe someone is trying to deceive you. REPORT THEM THROUGH OPPD's SUSPICIOUS EMAIL REPORTER BUTTON FOUND INSIDE OF OUTLOOK MAIL. Companies can also implement additional verification requirements for things like wire transfers or changing their procedures around ACH deposit changes. You can also consider adopting an additional step of authentication for access to email accounts. Pay attention, look for the signs, and implement best practices around multi-factor authentication which will help to protect your organization from becoming the next headline relating to CEO fraud.

Read more at:
https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/here-is-an-email-thread-of-an-actual-ceo-fraud-attack/

Don't be APRIL FOOLED

Avoid ID Theft & Tax Scams

Beware of unsolicited phone calls or emails.

- Scammers use scare tactics.
- Scammers demand immediate action.
- Scammers threaten arrest or court action.

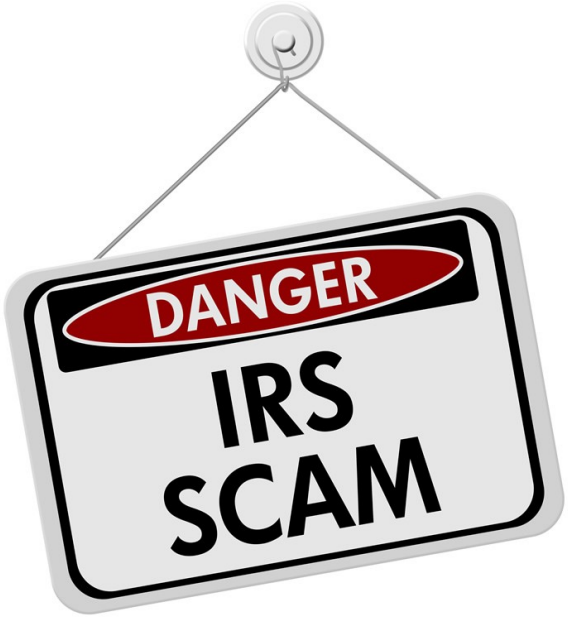
Don't give out personal information.

- Don't talk to them.
- **Hang up!**
- Don't open Attachments.
- **Hit delete!**

The IRS **doesn't initiate** contact with taxpayers by email, text messages or social media channels to request personal or financial information. To recognize the telltale signs of a scam visit the IRS webpage for tips and guidelines on fraud detection.

https://www.irs.gov/newsroom/how-to-know-its-really-the-irs-calling-or-knocking-on-your-door

Scam of the Week: IRS warns of new tax-related phishing scams



Every year we hear about tax fraud, people filing your taxes for you and then pocketing your refund before you even know it.

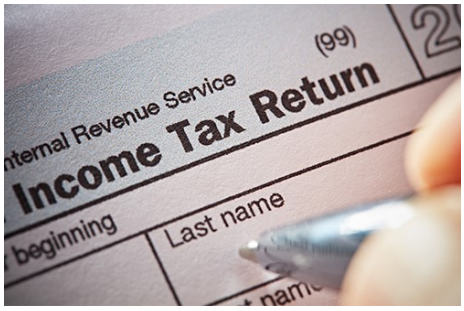
With tax season in full the IRS warns of new tax-related phishing scams swing the IRS us warning citizens, tax preparers, HR personnel and payroll staffer of new tax phishing tax scams being implemented this year by cybercriminals.

So far this tax season the IRS has come across a steady stream of fake emails, text messages, websites and social media attempts to steal personal information, most of which claim to be from the IRS. One new variation spotted actually has the malicious actors depositing money into the victim's legitimate bank account.

"After stealing client data from tax professionals and filing fraudulent tax returns, these criminals use the taxpayers' real bank accounts for the deposit. Thieves are then using various tactics to reclaim the refund from the taxpayers, and their versions of the scam may continue to evolve, IRS reported.

In this case the scammer usually phones the victim to pressure them into releasing the funds.

Human resources and payroll departments are also being hit with business email compromise scams to obtain W-2 information from their files so they can file fraudulent tax returns. These email generally pose as someone in authority at a business or organization who asks for the W-2 info on its members.



The IRS said tax preparers should also be on the watch for unsolicited emails from their customers, personal or business contacts. These could contain malware that will exfiltrate tax information from the target system. This type of attack is expected to be of particular concern this year because a huge numbers of names and email addresses have been stolen and are available for use by cybercriminals.

Any suspected email received should be forwarded to the IRS at phishing@irs.gov.

"Taxpayers should be on constant guard for these phishing schemes, which can be tricky and cleverly disguised to look like it's the IRS," said IRS Commissioner Chuck Rettig. "Watch out for emails and other scams posing as the IRS, promising a big refund or personally threatening people. Don't open attachments and click on links in emails. Don't fall victim to phishing or other common scams."

https://www.scmagazine.com/home/security-news/phishing/irs-warns-of-new-tax-related-phishing-scams/