# Tax Phishing Risks

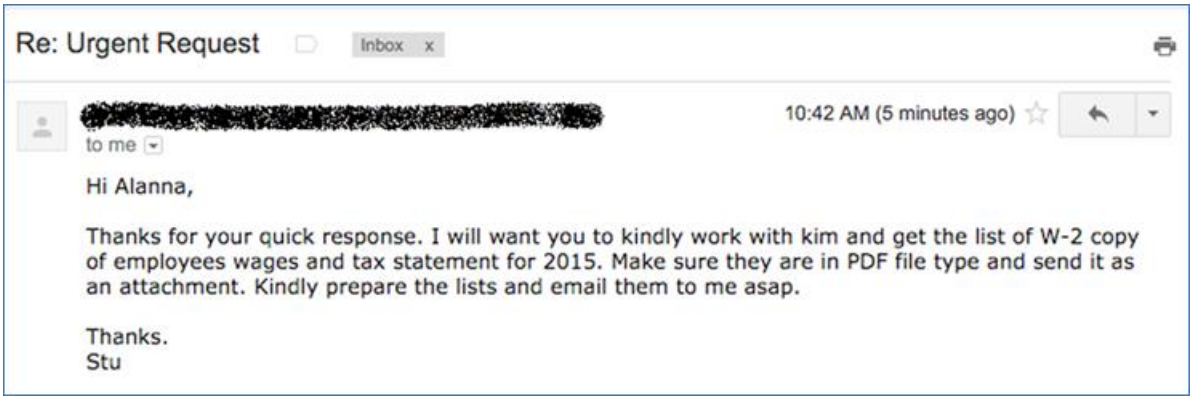
With everyone being in the midst of tax season, it's a good opportunity to send out a quick educational email on one of this season's most common phishing campaign topics: **taxes**. As you may know, tax season is one of the most popular time of year for scammers to start sending out phishing emails targeting personal and company-wide tax information.

One of the most common methods that a social engineer will use when sending out emails around tax season is to impersonate the IRS. Tax scam emails could direct recipients to fake tax forms, request fake tax payments or attempt to confirm tax submissions. We also need to keep an eye out for less obvious attacks. In the previous years' tax season, we saw many companies fall prey to CEO or upper management fraud, meaning the social engineer impersonated the target company's CEO or another member of upper management, rather than impersonating the IRS, requesting tax information for all employees. The tricky part of this type of email is that they often spoof the CEO's exact email address, making the email quite a bit more difficult to identify as fraudulent.

There are several things to consider when trying to protect ourselves from these types of phishing campaigns. Our first resource comes straight from the official IRS website, which states: "REMEMBER: The IRS doesn't initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information. In addition, IRS does not threaten taxpayers with lawsuits, imprisonment or other enforcement action. Being able to recognize these tell-tale signs of phishing or tax scam could save you from becoming a victim." Knowing this allows us to easily identify a great number of phishing campaigns that we could potentially receive during this time of the year.

Some other items to consider when trying to prevent yourself from falling prey to a phishing scam is to:

1. **Beware of typo's, bad grammar and misspellings**. A common theme in phishing campaigns are typos, misspellings, and grammatical mistakes, and these items may be one of your simplest identifiers.
2. **Be hesitant when following provided links**. If possible, type the address you know into your address bar, as the address you see in your email is not always where you end up.
3. **Report phishing emails that you have identified**. This step is often overlooked, but if you have received a phishing email, there is a good chance that someone else in the organization has received that same email. Just because you have identified that email as a phishing email, does not mean everyone else will. The best method to assure everyone is safe is to report the email to management (take a snapshot, do not forward live phishing emails).
4. **Verify the email is legitimate through a phone call to the sender**. Pictured below is a phishing email received by our friends at KnowBe4 during last year's tax season. While it spoofed the CEO's actual email address, even if we are unable to identify any obvious mistakes, we can acknowledge this is a lot of information to request through email. A 20-second phone call for confirmation is well worth the effort.
5. **When in doubt, click the "Reply" button**. If you receive an email from "yourceo@yourbank.com" that seems suspicious, clicking the "Reply" button will show your reply will be sent to "badguy@hackyou.com," revealing the email address has been spoofed.



Re: Urgent Request Inbox x

[redacted] 10:42 AM (5 minutes ago)

to me

Hi Alanna,

Thanks for your quick response. I will want you to kindly work with kim and get the list of W-2 copy of employees wages and tax statement for 2015. Make sure they are in PDF file type and send it as an attachment. Kindly prepare the lists and email them to me asap.

Thanks.
Stu