ADP Email Spam Alert - Check Your Whitelist

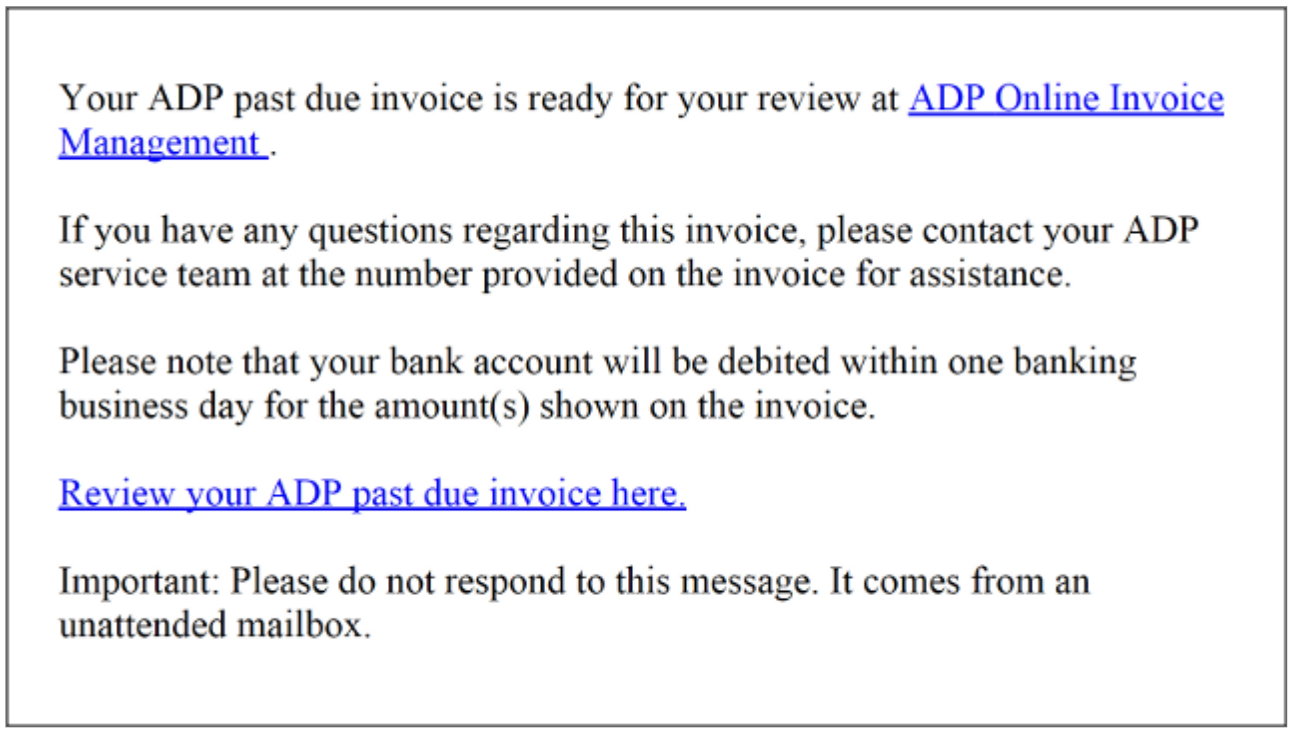
Spam News
By SteveG 11/13/2014

We blocked a big wave of ADP spam yesterday. The messages are "spoofed" (/blog/print/spam-news/adp-email-spam-alert-check-your-whitelist#what-is-spoofing) to look like they were sent from the company ADP, and include links that take you to dangerous web pages. If you get any of these emails, do not click the links.

We suspect that at least some people who received it have "whitelisted" ADP in their antispam programs to indicate emails from that company are to be trusted. That's the problem with whitelisting; it can easily be fooled.

About This ADP "Past Due Invoice" Spam

The campaign hit the first thing in the morning and we fully blocked it within a few minutes. The emails look very simple, just text about a past due ADP invoice that is ready for review, with links the spammer wanted you to click. We call those the "click-me" links that are common in spam. Here's a screen shot:



Your ADP past due invoice is ready for your review at ADP Online Invoice Management .

If you have any questions regarding this invoice, please contact your ADP service team at the number provided on the invoice for assistance.

Please note that your bank account will be debited within one banking business day for the amount(s) shown on the invoice.

Review your ADP past due invoice here.

Important: Please do not respond to this message. It comes from an unattended mailbox.

This simple-looking spam email actually quite dangerous

Do NOT click any of the links in the email. More on that next.

How Protect Yourself from this Spam

As soon as we saw this campaign, we blocked it based on several factors. Sometimes we do reveal our blocking techniques, but in this case, we don't want to make it any easier for the spammers due to the unique nature of the campaign.

More importantly, this spam is a good example of why you should not use whitelisting (https://www.spamstopshere.com/blog/email-security/whitelist-dangers-and-cyber-security). The spammers spoofed the header to make it look like the email address came from ADP, which is a company that probably a lot of people whitelist. If so, this dangerous email will bypass spam filters, even our own. So, you should probably review your spam settings to make sure ADP is not whitelisted.

> We do make whitelists and blacklists available to our customers, but we discourage their use outside of some specific situations. Most of our users heed our advice and never find a need to use either. When the need does arise, our support staff is happy to help customers makes entries that are narrowly tailored to the purpose. For example, some users may need to blacklist a stalker or whitelist a known contact from a country that is otherwise blacklisted.

What About SPF and DKIM?

> If you aren't familiar with SPF and DKIM, they are email validation systems that are supposed to prevent spoofing. When enabled, your email server can determine if the email domain in the header's from address (e.g., @example.com) came from a server authorized to send such emails.

Without getting into the details, these are valuable tools in the fight against spam, but they are not silver bullets. Used by themselves, they can greatly increase the number of false positives, making you spend much more time checking your junk folder (or quarantine) for legitimate email that was blocked. Also, whitelisting that domain will bypass any SPF or DKIM checking on most antispam systems, which completely defeats purpose of those validation tools.

We make SPF and DKIM, as well as other filtering tools, available to our customers, but we discourage them from doing any tuning, and most never do. Our 24/7/365 threat analysts (actual humans) use the validation technology as part of our arsenal and they rarely employ it by itself. They usually use it along with other filter rules to determine if an email is spam or not without increasing our incredibly low false positive rate.

What is Spoofing?

And Why It Makes Whitelisting Dangerous

Every email includes a "header" that you normally don't see unless you choose to view headers. Among other things, the header identifies who sent the email in the "From:" line, which looks something like this:

```
<From: john.doe@example.com>
```

That gets converted into the "From" address that you normally see.

So, it's easy for a spammer to put a fake address in there to make you think the email came from somewhere legitimate, like your bank, a popular retailer, or in this case, ADP.

That's called "spoofing", and it's one of the reasons we discourage the use of "whitelisting". A whitelist is is simply a list of email addresses and domains that you consider to be safe senders. Many antispam programs support them, so spammers spoof emails like this one to bypass your spam filter, which ends up increasing the amount of spam you get if you're not careful.

If you must whitelist, you can learn best practices in our article about whitelist dangers (https://www.spamstopshere.com/blog/email-security/whitelist-dangers-and-cyber-security).

Back to Top (/blog/print/spam-news/adp-email-spam-alert-check-your-whitelist#)

For More Info

SpamStopsHere works differently from other anti-spam programs. It blocks 99.5% of spam while delivering over 99.999% of legitimate emails. That means we block fewer that 1 out of 100,000 good emails, which is why businesses and professionals love our service.

Our spam review team, along with our proprietary Spamalyzer 3.0, analyzes and blocks email threats for our customers 24/7/365. That's a claim almost no other antispam provider can make.

Click here for more about SpamStopsHere and our 24/7/365 live support (https://www.spamstopshere.com/)