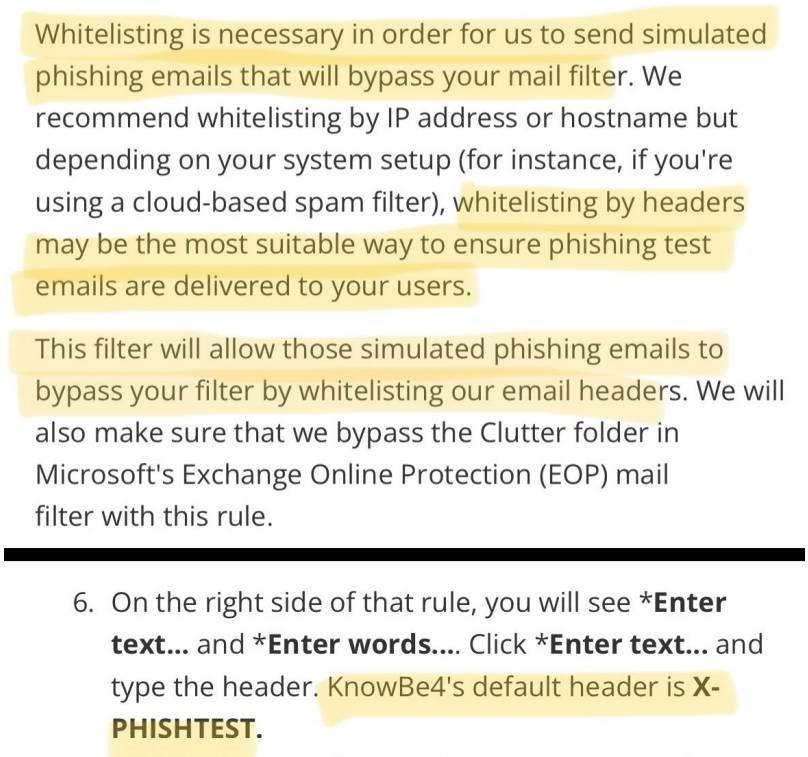
_MG_ **@_MG_** *Sat Dec 18 03:19:50 +0000 2021*

KnowB4 customers are some of the easiest to spearphish. This is just one example of why.

Their official instructions tell customers to setup filter bypasses that any attacker can also use. In the instructions, they include absolutely no cautionary info about it. ■ **https://t.co/gmHSz6MS6i**



Whitelisting is necessary in order for us to send simulated phishing emails that will bypass your mail filter. We recommend whitelisting by IP address or hostname but depending on your system setup (for instance, if you're using a cloud-based spam filter), whitelisting by headers may be the most suitable way to ensure phishing test emails are delivered to your users.

This filter will allow those simulated phishing emails to bypass your filter by whitelisting our email headers. We will also make sure that we bypass the Clutter folder in Microsoft's Exchange Online Protection (EOP) mail filter with this rule.

6. On the right side of that rule, you will see ***Enter text...** and ***Enter words...**. Click ***Enter text...** and type the header. KnowBe4's default header is **X-PHISHTEST**.

Phish Sim like knowbe4 is very often executed horribly, like what is seen below. Most of the time, it's used to send "gotcha" emails that are nothing like what actual attackers are sending. **https://t.co/r01bn7nYO2**

If anyone would like to validate the screenshot from my first post: **https://t.co/hU4erBTXYY https://t.co/xRmzCrTPf4**

It's not like this is a secret. Knowbe4 just doesn't care. They claim to have 30k customers. It's easy to find them: **https://t.co/rAsMYJF7yP**

And as you can see, this isn't the first time attention has been put on this. Knowbe4 just doesn't care.

It's their customers are quite literally the Last To Know thanks to KnowBe4's docs & system design.

https://t.co/yWX7lTntkv

The real poetry here is how this mirrors the impact of most phishsim programs when it comes to the education & psychology side. Most are teaching employees to take the bait of real attackers while wasting energy, time, & good faith that could have been used for positive change.

the irony **https://t.co/seYhdfy0oa**

It's been going on for years. I really do mean it when I say KnowBe4 customers are the Last2Know. **https://t.co/cdqFokKo0Q**

Even if your phish sim isn't opening a backdoor on your email system, it's most likely opening a backdoor into user behavior.

Check out this study that just dropped

https://t.co/6YwHdCPEid https://t.co/reWFuROtPu

The results of our experiment provide three types of contributions. First, some of our findings support previous literature with improved ecological validity. One example of such results is good effectiveness of warnings on emails. Second, some of our results contradict prior literature and common industry practices. Surprisingly, we find that embedded training during simulated phishing exercises, as commonly deployed in the industry today, does not make employees more resilient to phishing, but instead it can have unexpected side effects that can make employees even more susceptible to phishing. And third, we report new findings. In particular, we are the first to demonstrate that using the employees as a collective phishing detection mechanism is practical in large organizations. Our results show that such crowd-sourcing allows fast detection of new phishing campaigns, the operational load for the organization is acceptable, and the employees remain active over long periods of time.