



FINDING AND REMOVING JUST ONE PHISHING EMAIL IS A PAINFUL PROCESS






Threat actors are launching thousands, if not millions, of new phishing emails every single day. Detecting and remediating all those

phishing emails is an endless cycle

of tedious and time-consuming work for email security administrators.



EMAIL ADMIN IS FIRST ALERTED to a potential phish in various ways

-  End-user hits a **"report"** button
-  End-user forwards the **suspicious message** to the email admin directly
-  Email admin stares at their SEG dashboard, looking for **unusual messages or spikes** in email activity



EMAIL ADMIN REVIEWS THE SUSPICIOUS EMAIL



in different ways, depending on their environment



If they have a SEG

They review the email from their SEG dashboard; if they have a hybrid environment (mix of on-prem and cloud), they will have to do this research in the SEG protection in each type of environment. The admin has no way of knowing if the suspicious email is part of a larger polymorphic attack (i.e., an attack targeting end-users with emails that have identical/similar content).



If they have O365

The admin can review the email in Microsoft eDiscovery or delivery logs. They can also search with PowerShell or the Defender dashboard. Unfortunately, different pieces of information are available in each tool, so it is up to the admin to make sense of it. The admin must search for each individual phishing email, as they aren't clustered in any of these Microsoft tools.

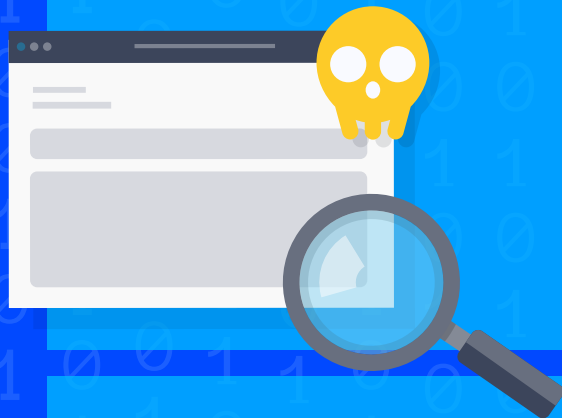


If they have GWS

The admin has two main ways to investigate – the Security Investigation Tool or Google Apps Manager (GAM), which is a command-line tool known to most GWS admins. As with the Microsoft tools, the GWS tools do not cluster like or similar phishing emails.



EMAIL ADMIN CONDUCTS A "SEARCH AND DESTROY" MISSION



Once the email admin determines that the suspicious email is in fact a phishing attack, they must then use the tools available with their email technology to conduct a "search and destroy" mission on an email-by-email basis to **get them out of the end-users' inboxes...**and hope that they didn't miss any.

EMAIL ADMIN RECORDS THE TIME AND SCOPE OF THE INCIDENT



To ensure that all this work is documented, the email admin will often need to **create/update a ticket** in their IT Service Management (ITSM) tool to record the time and scope of the incident.



So, that's one phishing email resolved.

On to the next one

