

Phishing is for real. \$5.3 Billion was stolen due to Business Email Compromise between 10/13-12/16. By comparison, \$1 Billion was lost due to ransomware in 2016, per the Internet Crime Complaint Center.

It's not a matter of if...

Is the identity of your colleagues already compromised? Are attackers lurking in your email accounts? **Most organizations only become aware of a breach when end-users or customers notice.**

The Challenge:

Users may avoid obvious phishing scams, but attackers are organized and patient.

Most email impersonation occurs long

after a breach. During that time, an attacker learns to craft the perfect message to the paying victim.

For IT Pros, Microsoft's identity and email tools offer robust logs and policy controls. Yet sifting through all the information to find a rare breach is time consuming. **A shorter, actionable set of steps is needed.**

Enabling Technologies' Solution

We combine Microsoft's tools and our forensic knowledge to analyze threats, customize rules, and automate responses to targeted attacks. Admins will get a short list of actionable next steps, and users are left with a clean inbox and less risk. The solution is called **Phish Hunter**, and is configured in each tenant to **minimize business email compromise.**

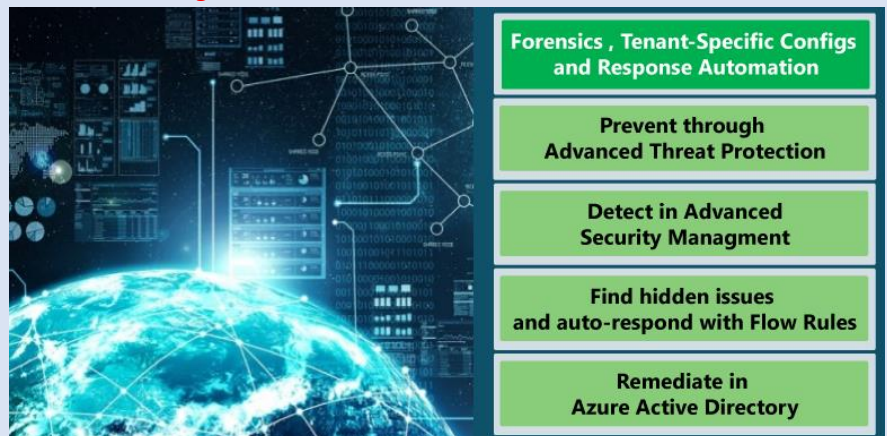
To Go on the Hunt

Please contact securecloud@enablingtechcorp.com for a **forensic assessment** of your Office 365 tenant. If issues or risks are present, we'll provide guidance for setting up Phish Hunter to **remediate or proactively block breaches** in the future.

Actual losses from affected organizations come in big chunks, shown below



Phish Hunter gives admins a short list of automated actions to remediate



There's no reason to delay, the big phish just may not have bitten yet.

