Barracuda Email Threat Scanner for Office 365

https://campus.barracuda.com/doc/78807326/

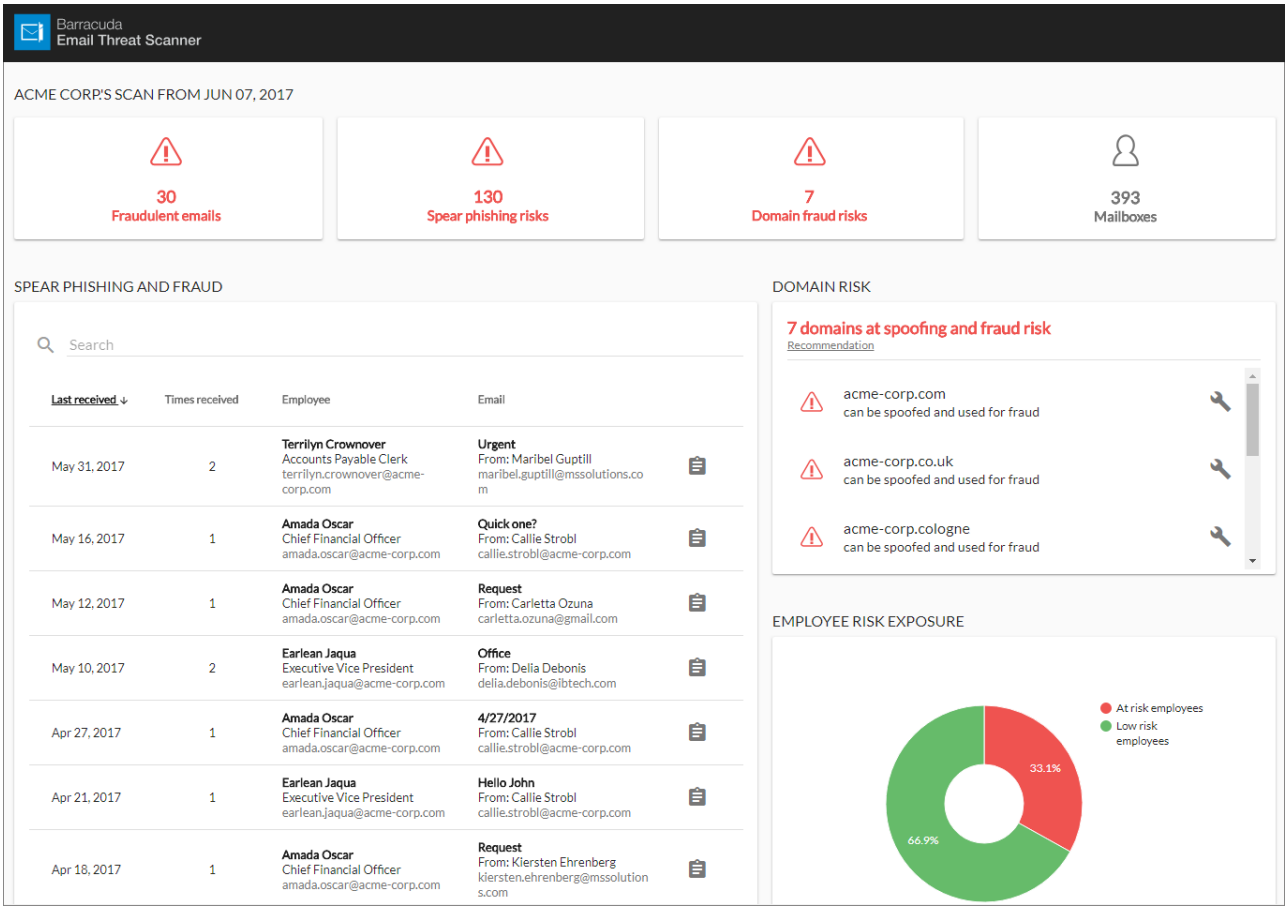
Use the free Barracuda Email Threat Scanner for Office 365 to discover spear phishing and targeted attacks that reside in your Microsoft Office 365 account. This web-based service uses Barracuda Sentinel's Artificial Intelligence engine to scan your Office 365 accounts for spear phishing attacks that are currently sitting in user mailboxes. The cloud-based scan runs in the background and identifies mailboxes that contain risks including who the mailbox belongs to, the sender of the risk, and details about the risk including what the risk is targeting. The service scans for:

- Spear phishing attacks
- CEO fraud and employee impersonation
- Popular web service impersonation (Outlook, DocuSign, Dropbox, Apple)
- Account takeover attempts

It takes two minutes to sign up for the scan, and the scan typically completes within 24 hours.

Scan for Threats

1. Go to https://scan.barracudanetworks.com, and enter your Barracuda Cloud Control account credentials in the associated fields. Review the **Barracuda Privacy Policy**. You can create an account, and then click **Get Started**, or click if you have a Barracuda Cloud Control account, click **I already have a Barracuda account**, and click **Sign In**.
2. Click **Connect Office 365 to Scan Your Account**; you are prompted to log in to your Office 365 account. Enter your admin login credentials, and click **Sign in**.
3. Review the requested permissions, and then click **Accept**.
4. Once permissions are accepted, **Barracuda ETS for Office 365** displays. Click **Start Threat Scanner**.
5. Barracuda Email Threat Scanner for Office 365 immediately begins scanning your Office 365 account for threats.
6. Once the scan is complete, the Scan report displays threats found within your emails and domains:



7. For suggestions on resolving at risk domains, click the **Suggestion** (🔧) icon in the **Domains at Risk** section.
8. To determine the number of employees found at high versus low risk, mouse over the graph in the **Employee Risk Exposure** section.

Once threats are identified, Barracuda recommends deploying Barracuda Sentinel for real-time spear phishing and cyber fraud defense. For more information, see Barracuda Sentinel.

Figures