Microsoft CyberSecurity Awareness Kit

From Microsoft and Terranova Security

In response to rapidly-evolving customer needs, Microsoft is releasing a cybersecurity awareness kit in partnership with Terranova Security. This kit contains three full end user phish and privacy education courses, two videos about the coronavirus-themed attacks, and several blog posts, posters, newsletters, and infographic sheets. We are providing this to all of our customers so that they can educate their organizations and reduce phishing risk during this time.

The kit contains one zip file, and links to three courses that organizational administrators can distribute to their end users, if they choose. These courses are hosted online at the following locations, but are also included as HTML files in the zip files so that admins can deploy and manage those courses in whatever way is most efficient for their organizations. Deploying each unzipped directory to an Internet Information Server (IIS) hosted on an organizationally managed server takes only moments and provides admins with a lot more control over network access and authentication and authorization. If the admin chooses, they can distribute the below links to their end users as well. Any authenticated Microsoft 365 user should be able to take the courses here:

* <https://security.microsoft.com/attackSimulatorTrainings/covid19Trainings?covid19Training=massphishingtraining>
* <https://security.microsoft.com/attackSimulatorTrainings/covid19Trainings?covid19Training=protectinghomecomputertraining>
* <https://security.microsoft.com/attackSimulatorTrainings/covid19Trainings?covid19Training=privacytraining>

The zip file, named COVID19Kit.zip, contains the following items:

* MassPhishing-Training.zip. This course helps users understand how mass phishing campaigns work and how they can recognize them. Admins can deploy the HTML training course on a server they manage, or share the link to a Microsoft-hosted version here: <https://security.microsoft.com/attackSimulatorTrainings/covid19Trainings?covid19Training=massphishingtraining>
* ProtectingYourHomeComputer-Training.zip. This course helps users understand how and why threat actors go after their home computers, how that puts organizational information at risk, and what they can do to protect themselves at home. Admins can deploy the HTML training course on a server they manage, or share the link to a Microsoft-hosted version here: <https://security.microsoft.com/attackSimulatorTrainings/covid19Trainings?covid19Training=protectinghomecomputertraining>
* Privacy-Training.zip. This course helps users understand why their personal information is a target for hackers, and how they can maintain their privacy. Admins can deploy the HTML training course on a server they manage, or share the link to a Microsoft-hosted version here: <https://security.microsoft.com/attackSimulatorTrainings/covid19Trainings?covid19Training=privacytraining>
* COVI19PhishingScamsNanoTraining.mp4. This short video explains how COVID19 is being used as a lure in phishing scams. Admins can distribute this video with their organizations by uploading it to a SharePoint document library and sharing a link with their organizations.
* COVID19WebScamsWebcast.mp4. This webcast, hosted by Terranova Security professionals dives deeper into Covid-19 themed phishing campaigns. Admins can distribute this video with their organizations by uploading it to a SharePoint document library and sharing a link with their organizations.
* Blogs and Infographics Folder. This folder contains several PDF files of blog posts and informational data sheets about fraud, privacy, working from home, and COVID19-themed phishing campaigns. Admins can distribute these files to their organizations by uploading it to a SharePoint document library and sharking a link with their organizations.
* Fraud and Privacy Posters and Newsletters. These two folders contain PDFs of short, at-a-glance guidance on how to avoid common pitfalls of phishing scams. Admins can distribute this files to their organizations by uploading it to a SharePoint document library and sharking a link with their organizations.
* End User License Agreement governing your use of all the material in the kit.

Microsoft is making these resources available to all of our customers for free for a period of at least three months. Your use of these resources is governed by the terms detailed in the End User License Agreement included in the zip kit. We hope you'll be able to leverage this kit to educate and inform your organization so that you can stay safe from all the risks associated with COVID19, including how it is being used in phishing campaigns.