

# Pre-Deployment

Last Modified on 09/15/2023 2:35 pm CDT

## Minimum System Requirements

### iLMS and Courses

#### Browsers for Windows OS

Chrome 75+

FireFox 66+

Edge 89+

#### Browsers for Mac OS

Safari 13.0.2+

Chrome 75+ (Only supported for Courses with Engine v 5.1.3 +)

#### Browsers for Linux OS (Only supported for Courses with Engine v 5.1.3 +)

Chrome 75+

FireFox 66+

- JavaScript must be enabled/allowed in the browser in order for courses and platforms to operate.
- Required bandwidth per host machine of 4Mbps download and .5Mbps upload is required
- iPad access is supported only for HTML5-based courses in the latest version of iOS with Safari
- Courses are best viewed with a browser and OS zoom level of 100% and a display screen resolution between 1024 x 768 and 1920 x 1080.
- Inspired eLearning **does not** officially support training taken using the following:
  - Mobile Web Browsers on Smartphones
  - Thin clients (Citrix/Virtual Desktops),
  - VPN connections
  - Proxy connections

### Identifying the version of Inspired eLearning's Course Engine

To identify the version of the Course Engine used by your course, you can launch the course and look at the lower right-hand corner of the player.

Shown Here:



## iLMS LDAP Connector requirements

Windows operating system with Net Framework v4.6.2 and above

## PhishProof and Phishhook Add-in

### Supported Email Clients for Phishproof Campaigns:

Microsoft Outlook 2003+, Hotmail, Gmail, Yahoo Mail

### PhishHook Add-in Minimum System Requirements:

- MS Office 2010 - Outlook Desktop Client
  - MS Office 2016 on Windows is not supported
- Microsoft VSTO 2010 Runtime
- .Net v4.5 framework

If your organization would like to use Phishproof's Outlook add-in Phishhook, which will allow users to report suspected phishing attempts, we recommend having your IT team roll this feature out prior to deployment.

This can be installed centrally via the *MS Office 365 Admin Console*

Full Phishhook Setup Instructions Here: [Phishhook Add-In](#)

**Note:** PhishHook is not supported for On-Premise Exchange environments

## Pre-Deployment Action items for iLMS

To ensure that the iLMS and courses will function properly the following items need to be completed.

**Add the following domain names to the allowlist on your Intrusion Detection System, and if necessary, your firewall:**

LMS Domain:	inspiredlms.com
StatZen Domain:	<a href="#">securityawarenesstraining.com</a>
CDNs for Course Content:	spa.tclcdn.com inspiredcdn.s3.amazonaws.com assets.tclcdn.com

To allow Email communication from LMS to end user, please add the following domains to the allowlist on your email filter:

Default LMS Sender Domain:	*.inspiredlms.com
Domains used for communications from Inspired internal teams to Designated Organization Contacts	*.inspiredelearning.com *.vipre.com
Domain used for reporting from StatZen Reporting tool:	*.securityawarenesstraining.com
Domain used for communication with our support teams	*.inspiredelearning.zendesk.com

Add the following to the trusted sites and privacy settings in Internet Explorer:

LMS Domain	*.inspiredlms.com
(Only If using Skillsoft Content) Content Streaming Domain	www.skillport.com

Allow pop-ups from the following site as pop-up blockers will prevent the course from launching:

LMS Domain	*.inspiredlms.com
------------	-------------------

If your organization would prefer to add to the allowlist by IP as opposed to domain, please inform your account manager to receive that information.

---

## Pre-Deployment Action Items for Phishproof

We will be sending simulated phishing emails from outside your network, so your IT department must be notified.

Please ensure your environment meets the following criteria for compatibility:

- Email client(s): MS Outlook 2003+, Hotmail, Gmail, Yahoo Mail
- Browsers: Chrome 71+, FireFox 65+, IE 9+, Safari 11.1.2+

If your organization plans to use the optional add-in, Phishhook, to allow users to report suspicious emails, please ensure the environments meets the following criteria.

### PhishHook Add-In Installation Requirements

- MS Office 2010
- Microsoft VSTO 2010 Runtime
- .Net 4.5 framework

In order for emails to be delivered successfully to the end-user, please perform the following allow-listing tasks:

This may be required in the locations listed

- Intrusion Detection System/Firewall
- Client-side Email Filters
- Server-side Email Filters

**Note:** For Organizations using Microsoft email services, there have been changes to allow-listing requirements. Regular rules will no longer allow through emails that look like spam even if they are added allowed senders.

There is a new location Microsoft requires exceptions to be made for Phishing simulations. This was added as of July 2021.

Please see the Microsoft article here for more information: [Configure 3rd Party Phishing Simulations in Microsoft 365 Defender Portal](#)

Microsoft customers may also need to set up rules to bypass ATP's link and attachment processing. Instructions on how to create a bypass rule can be found here: [Phishproof: Microsoft ATP Bypass Rules](#)

**Allowlist the following domain name of the SMTP relay used by the application.**

SMTP Relay:	smtp.mailgun.org
-------------	------------------

**Allowlist the following location that hosts the landing pages in your web filtering software, if applicable.**

Landing Page Domain:	*phishproof.com
----------------------	-----------------

**Allowlist the following domains used when sending Phishproof Email Templates:**

<b>Template Domains:</b>	accountsecurity.online amznbks.com bankameriica.com certifyjob.com clickweb.solutions facebookfriendster.com filescanners.org formsmail.com funitgames.org googlesecurity.net ibsbanks.com mailsystems.online phishproof.com securityadmin.net securityalert.org starrwood.net systemadmsmin.org twittersocialpage.com upssite.com uspostallservice.com wallgreenspharm.com web-access-alerting.com boxfilesshare.com docutransfers.com employee-rewards.net hr-rewardscenter.com hq-administrators.com itpatching-installs.com corp-addmin.com admin-tokenalert.com sso-server.com login-microsoft.com
--------------------------	--

**Note:**

Security Features such as websense/zscaler, rate limiters, dynamic email filters, and/or Googlebot that click on links before the users will need to be filtered in the Phishproof application's admin portal.

This can be done by following instructions here: [Phishproof Filter Bots](#)

Adjusting any other settings, as necessary, to ensure the simulated phishing emails flow to end-user inboxes.

If your organization would prefer to add to the allowlist by IP as opposed to domain, please inform your account manager to receive that information.

Additional things to consider:

- Do employees have general access to the internet?
- What kinds of work stations/devices have permissions to access email?
- Do users have the ability to play MP4 videos? (Education landing pages may include video)

