# Graphus Introduction to End-Users (Employees)

**Subject:** Advanced Email Security Rollout

Dear Colleague,

We have recently activated an advanced email security solution named Graphus to protectyou against sophisticated email attacks.

As you may be aware, email attacks are the number one reason for network and data breaches. These sophisticated attacks leverage social-engineering tactics to trick users into replying to an email, clicking a link, or opening an attachment. Such user actions ultimately result in the loss of money or confidential information, a system being infected with malware/ransomware, or an email account being taken over.

The Graphus solution will automatically quarantine malicious emails, preventing them from reaching your inbox. If Graphus determines an email is suspicious but that it also could be legitimate, it will insert an interactive warning banner in the email. The banner includes information about the specific threat detected in the email and provides the opportunity for you to act on it.



After reading the warning message, if you agree that the email is indeed a threat, click **Report Phishing**. You might be required to authenticate to validate you are the intended recipient of this email. The email will automatically be removed from your inbox and your IT Security team will be notified. However, if you are certain the message is not suspicious, click **Mark as Safe** and the banner will disappear from the email.

The banner will include an option to mark an email as junk. If you determine an email is not suspicious, but you don’t want to receive future emails from this sender, you can click the **Block as Spam** link.

Providing explicit feedback by clicking **Report Phishing** or **Mark as Safe** protects our organization in real-time from sophisticated email attacks. And doing so enables the system to “learn” how to treat future emails from the sender. Your active participation is much appreciated.

### Phish911 (Option 1 – Forward email)

If you see an email that looks suspicious but does not have a banner, you can still report that message to us by forwarding that email to <*user-reported-email- address*>. When you forward an email to this address, it will be immediately removed from your inbox and your IT team will be notified for further action.

## Phish911 (Option 2 – Microsoft Outlook client)

### Using Report Message add-in

If you see an email that looks suspicious but does not have a banner, you can still report that message to us by selecting **Report Message > Phishing** in the Microsoft Outlook client. The email will be removed from your inbox and your IT team will be notified for further action.

### Using Report Phishing add-in

If you see an email that looks suspicious but does not have a banner, you can still report that message to us by selecting **Report Phishing** on the Microsoft Outlook client ribbon. The email will be removed from your inbox and your IT team will be notified for further action.

## Phish911 (Option 3 – Microsoft Outlook on the Web)

Using Report Message add-in or Report Phishing add-in

If you see an email that looks suspicious but does not have a banner, you can still report that message to us by selecting **Report > Report phishing** in the Microsoft Outlook web application. The email will be removed from your inbox and your IT team will be notified for further action.

If you have any questions, please contact <name> at <email address>.