Item	Channel	Details	Delivery Date
Email to Pilot Groups	EASI Information Security Selected A&S Selected HR Engineering ACE-IT Group Members of ACT, UTM, UTSC		Week of March 23 - complete
Email to IT Groups	Infotech Listserv EITU listserv	Ensure departmental emails aren't being marked as external	March 30 - complete
Email to expand Pilot Group	Senior Leadership within Simcoe Hall - pilot group Central communications DUA SGS Student Life OISE Enrolment Services Faculty Key Comms contacts: A&S, Engineering, Architecture, Dentistry, Information, Forestry, Law, KPE, Music, Nursing, Pharmacy, Social Work, Medicine, Theology Colleges: Victoria, University, Trinity, Innis, Woodsworth, St. Mike's, New College Accessibility Services Procurement	Ensure departmental emails aren't being marked as external Suggestions for other participants --> its-pilot-feedback@utoronto.ca	March 31 - complete

	FAST Rotman Indigenous Services CIE Libraries Hart House Student Unions		
Notifying Students – Briefing Note Review and Approval	Create briefing note for registrars and sample email to students		May 14 - complete
EASI web presence – with information about project	O365 – Outlook – Get Help https://easi.its.utoronto.ca/shared-services/office365/utmail/		May 14 - complete
Email to expand Pilot Group	Shared Services	Ensure departmental emails aren't being marked as external	May 21 - complete
Notified Info Commons – Help Desk	Asking Help Desk to triage questions from students – submit an ESC ticket on their behalf		Confirmed
Notify Student Societies and Student Life		Ensure student society emails aren't being marked as external	July 7 - complete
Additional IT Team members SCS			July 8
Notify Registrars	Registrars' listserv	Initial notice about the project if they haven't heard of it already	July 9
UTM	Notify clients at UTM – within next 2 weeks They will handle comms		• Week of July 20 - enroll first group of early adopters (157) • Week of August 18 - enroll rest

			of administrative staff and research assistants (122) • September 30 – full deployment
MailChimp Senders	If you don’t have sender authentication enabled, your emails will get the banner – need to be exempted		September 14 - complete
UTSC			September 30 – full deployment
A&S	Phased approach 1. IITS and central offices 2. Admin departments 3. Academics They will handle comms		A&S Notified IT Departments
Notification that general message is going out	ACE IT (meeting) EITU (meeting) Infotech (September 23 – email)		Cathy/Isaac to speak at ACE IT meeting September 23 EITU Meeting September 23 Infotech Email September 23 - Complete
UTSC UTM	UTSC (done) and UTM (done) - confirmed		Week of September 21 - complete
Notifying Students	Enrollment Services (social media) - confirmed – sent to registrars Student Life (social media/newsletter) - sent ACORN Launchpad - Navi and COVID messages are taking priority		September 24 afternoon (September 30 – full deployment) - Complete

	Quercus? (advised there are very few global messages posted and they need to be reviewed by an executive steering committee) - sent A&S (social media/newsletters) - confirmed – social media and newsletter		
General/Broad Announcement	EASI Website • News article In the Loop (link to the EASI news article) + ITS social media ServiceNow Knowledge Base Article ITS Website – announcement on homepage and banner • CISO page - link to info • Security Matters website – link to info Help Desks – coordination Email to Registrars – Reminder Communications listserv – Reminder (September 30)		September 24 - complete
Email to Infotech with preview instructions and update on project	Infotech Listserv	• Goal of project/importance • FAQs/resources to answer questions • Pilot • If you need to have email sources exempted (not individuals), visit https://uoft.me/eeber	October 2 - complete

Update to EASI website – project page	https://easi.its.utoronto.ca/initiatives/external-email-banner-project/	• Goal of project/importance • FAQs • How to get help	October 2 - complete

Email to Pilot Groups (sent week of March 23):

Good morning,

In response to the increasing number of phishing attacks on the University of Toronto community, EASI's Office 365 team is evaluating the introduction of external email notification banners to all emails originating from outside the University of Toronto. The banner will serve to bring awareness for faculty, staff and students to be cautious when opening external emails and attachments.

As part of this process, we are launching a pilot project for the external email notification banner with a group of select users. Your name has been put forward by your division to participate as a pilot user.

The pilot will start shortly after the delivery of this notification, and you will see the banner below on external emails in your inbox (the formatting may differ slightly based on your client):

The banner will appear above the body text of an email and will state:

EXTERNAL EMAIL: Treat content with extra caution.

A valuable part of your participation in this pilot project will be your feedback: we ask that you provide feedback to its-pilot-feedback@utoronto.ca email address. Your comments will help us to ensure the external email banner meets the needs of the larger University of Toronto community.

We thank you in advance for your participation and ask that you contact its-pilot-feedback@utoronto.ca with any questions or concerns.

Sincerely,

EASI

Enterprise Applications and Solutions Integration

Email to IT Groups (week of March 30):

Dear colleagues,

Enterprise Applications and Solutions Integration and Information Security are currently running a pilot project to evaluate the introduction of external email notification banners for UTmail+ (Office 365) in response to the increasing number of phishing attacks on the University.

These banners will appear on all emails originating from outside the University of Toronto. They will serve to bring awareness for faculty, staff and students to be cautious when opening external emails and attachments that could be potentially malicious.

While we gather feedback from the project's pilot users, we also want to work with the University's IT community to ensure that departmental emails do not get marked as external. **We ask that departments submit the IP addresses of their email servers and information about Bulk Mailers (like SendGrid, MailChimp, etc.) that are in use to** its-pilot-feedback@utoronto.ca. This critical step will ensure that we exempt departmental emails from getting the external email banner.

Please respond by April 6.

We appreciate your assistance with this information gathering process. Please direct any questions or concerns to its-pilot-feedback@utoronto.ca.

Kind regards,

Enterprise Applications and Solutions Integration

Information Security and Enterprise Architecture

Email to Comms Contacts (sent March 31):

Hi everyone,

I hope you're doing well during these difficult times.

I wanted to touch base to include you in a pilot that Information Technology Services is running to introduce external email banners for U of T email (Office 365). The goal of this project is to decrease the amount of successful phishing attacks on U of T.

These banners will appear on all emails originating from outside U of T. They will serve to bring awareness for faculty, staff and students to be cautious when opening external emails and attachments that could be potentially malicious.

While we gather feedback from the project's pilot users, we also want to work with the university community to ensure that newsletters and collaboration tools (Asana etc.) do not get marked as external. **We ask that departments/units/colleges submit the IP addresses of their email servers and information about Bulk Mailers (like SendGrid, MailChimp, etc.) that are in use to** its-pilot-feedback@utoronto.ca. **by April 6.** This critical step will ensure that we exempt departmental emails from using the external email banner.

We appreciate your help with this process. Please help us spread the word with any colleagues who might be affected. Please direct any questions or concerns to its-pilot-feedback@utoronto.ca.

Thanks!

Email to Shared Services (May 21):

Dear colleagues,

Enterprise Applications and Solutions Integration and Information Security are currently running a pilot project to evaluate the introduction of external email notification banners for UTmail+ (Office 365) in response to the increasing number of phishing attacks on the University.

These banners will appear on all emails originating from outside the University of Toronto. They will serve to bring awareness for faculty, staff and students to be cautious when opening external emails and attachments that could be potentially malicious.

You will see the banner below on external emails in your inbox:

While we gather feedback from the project's pilot users, we also want to work with the University's IT community to ensure that departmental emails do not get marked as external. **We ask that departments submit the IP addresses of their email servers and information about Bulk Mailers (like SendGrid, MailChimp, etc.) that are in use to** its-pilot-feedback@utoronto.ca. This critical step will ensure that we exempt departmental emails from getting the external email banner.

We appreciate your assistance with this information gathering process. Please direct any questions or concerns to its-pilot-feedback@utoronto.ca.

Kind regards,

Webpage:

https://easi.its.utoronto.ca/shared-services/office365/utmail/

- Webpage links to:
    - ITS Website https://its.utoronto.ca/ – announcement on homepage and banner
    - CISO page – https://ciso.utoronto.ca/
    - Security Matters – https://securitymatters.utoronto.ca/

External Email Banner Project

Since March 2020, Enterprise Applications and Solutions Integration and Information Security have been evaluating the introduction of external email notification banners for UTmail+ (Office 365). This banner will help to protect U of T from hackers and phishing attempts, and will also protect our faculty, staff and students' valuable information.

Phishing emails often ask recipients to click on links or open attachments, and frequently appear to come from an internal senders. This warning banner will appear on all emails originating from outside U of T and will serve as a reminder to treat external emails with caution. Messages from legitimate U of T senders will not display the banner.

This is how the banner will appear at the top of your email:

To date, the project has spanned all three campuses and has gathered feedback from over 650 pilot users. The technical team has also worked with U of T's IT community to mark departmental emails as internal – departments have submitted the IP addresses of their email servers and information about bulk mailers like SendGrid and MailChimp.

We continue to expand the pilot across U of T in an effort to streamline the use of the banner and ensure accuracy.

If you would like to request an exemption, please submit a ticket via ESC using the following link: https://uoft.me/eeber

Have you received a phishing attempt? Click on "Report Message" in your email.

Reminders when clicking on links or opening attachments in emails:

- Ensure that the sender and email domain are legitimate
- Review the content and consider if the message typical for the sender
- Hover over links to review addresses before clicking
- Ensure you recognize the sender's name or department

Briefing Note and Sample Student Email:

Dear Name,

Since March 2020, Enterprise Applications and Solutions Integration and Information Security have been evaluating the introduction of external email notification banners for UTmail+ (Office 365). This banner will help to protect U of T from hackers and phishing attempts, and will also protect our faculty, staff and students' valuable information.

This warning banner will appear on all emails originating from outside U of T and will serve as a reminder to treat external emails with caution. Messages from legitimate U of T senders will not display the banner.

This is how the banner will appear at the top of your email:

To date, the project has spanned all three campuses and has over 650 pilot users. The technical team has also worked with U of T's IT community to mark departmental emails as internal – departments have submitted the IP addresses of their email servers and information about bulk mailers like SendGrid and MailChimp.

We continue to expand the pilot across U of T in an effort to streamline the use of the banner and ensure accuracy. As part of this expansion, we would like to notify students about this project through registrarial offices. We are hoping you can review this message below and provide any feedback before distribution.

****

Hi everyone,

Some of you may be familiar with U of T's external email notification banner for UTmail+ (Office 365). We hope you can help us distribute this message to your students to notify them about this important step in improving cybersecurity.

****

Dear student,

On [DATE], U of T will implement an external email notification banner for all UTmail+ accounts - @utoronto.ca and @mail.utoronto.ca accounts. This banner will help to protect you from hackers and phishing attempts, and will protect your valuable information.

Phishing emails often ask recipients to click on links or open attachments, and frequently appear to come from an internal source. This warning banner will appear on all emails originating from outside U of T and will serve as a warning to treat external emails with caution.

This is how the banner will appear at the top of your email:

Reminders when clicking on links or opening attachments in emails:

- Ensure that the sender and email domain are legitimate
- Review the content and consider if the message typical for the sender
- Hover over links to review addresses before clicking
- Ensure you recognize the sender's name or department

What to do if you receive a phishing attempt:

Click on "Report Message" in your email.

Notice to Student Societies

Dear student society leaders,

Since March 2020, the University has been evaluating the introduction of external email notification banners for UTmail+ (Office 365). The banner will help to protect U of T from hackers and phishing attempts and will also protect the valuable information of our students, staff, and faculty.

Phishing emails often ask recipients to click on links or open attachments, and frequently appear to come from internal senders. The banner will appear on all emails originating from outside U of T and will serve as a warning to treat external emails with caution. Messages from legitimate U of T senders will not display the banner.

This is how the banner will appear at the top of an external email:

If your society sends messages or newsletters directly through any external email system, including MailChimp, , please provide the name of the product and the email account to its-pilot-feedback@utoronto.ca. **This will ensure that the University exempts your society's emails from displaying the banner.**

If your society sends messages or newsletters through the U of T Listserv system (i.e., STUDENT_SOCIETY_XXX_L@LISTSERV.UTORONTO.CA), even if they are prepared in a bulk mailer platform, they are already exempt from displaying the banner.

We appreciate your assistance with this information gathering process. Please direct any questions or concerns to its-pilot-feedback@utoronto.ca.

Signature

Initial Notice to Registrars

Dear Colleagues,

Since March 2020, Enterprise Applications and Solutions Integration and Information Security have been evaluating the introduction of external email notification banners for UTmail+ (Office 365).This banner will help to protect U of T from hackers and phishing attempts, and will also protect our faculty, staff and students' valuable information.

These banners will appear on all emails originating from outside the University of Toronto. They will serve as a warning for faculty, staff and students to be cautious when opening external emails and attachments that could be potentially malicious.

This is how the banner will appear at the top of your email:

We are also working with the U of T community to ensure that departmental emails do not get marked as external. If you are using MailChimp, please set up Sender Authentication for your MailChimp account using the steps below. Authentication is a sender identification tool that protects email senders and their recipients from spam, forgery, and phishing. Additionally, it will help improve delivery rates for external recipients. If you are using any other external mail system, please provide the name of the product and the email account to its-pilot-feedback@utoronto.ca.

MailChimp Instructions:

- Login to your MailChimp account(s) and navigate to the Domains page in your Account Settings.
- Please ensure that the domain is Verified. You should see the word 'Verified' next to the domain name.
- Next to the verified email domain you want to work with click Authenticate.
- Click Authenticate Domain.

Once we've heard back from the community, we will be moving forward with this project by the end of this summer.

If you have any questions, please contact its-pilot-feedback@utoronto.ca.

Signature

Email to IT Contacts SCS:

Dear colleagues,

Since March 2020, Enterprise Applications and Solutions Integration and Information Security have been evaluating the introduction of external email notification banners for UTmail+ (Office 365).This banner will help to protect U of T from hackers and phishing attempts, and will also protect our faculty, staff and students' valuable information.

These banners will appear on all emails originating from outside the University of Toronto. They will serve as a warning for faculty, staff and students to be cautious when opening external emails and attachments that could be potentially malicious.

This is how the banner will appear at the top of your email:

While we gather feedback from the project's pilot users, we also want to work with the University's IT community to ensure that departmental emails do not get marked as external. If you are using MailChimp, please set up Sender Authentication for your MailChimp account using the steps below. Authentication is a sender identification tool that protects email senders and their recipients from spam, forgery, and phishing. Additionally, it will help improve delivery rates for external recipients. If you are using any other external mail system, please provide the name of the product and the email account to its-pilot-feedback@utoronto.ca.

MailChimp Instructions:

- Login to your MailChimp account(s) and navigate to the Domains page in your Account Settings.

- Please ensure that the domain is Verified. You should see the word ‘Verified’ next to the domain name.
- Next to the verified email domain you want to work with click Authenticate.
- Click Authenticate Domain.

We appreciate your assistance with this information gathering process. Please direct any questions or concerns to its-pilot-feedback@utoronto.ca.

Kind regards,

Enterprise Applications and Solutions Integration

Information Security and Enterprise Architecture

General Email to Staff SCS:

Dear colleagues,

Since March 2020, Enterprise Applications and Solutions Integration and Information Security has evaluated and introduced external email notification banners for UTmail+ (Office 365).This banner will help to protect U of T from hacking and phishing attempts, and will also protect our faculty, staff and students’ valuable information.

These banners will appear on all emails originating from outside the University of Toronto. They will serve as a warning for faculty, staff and students to be cautious when opening external emails and attachments that could be potentially malicious.

We have gathered feedback from all three campuses, and are now rolling this banner out to all remaining staff, faculty and students.

This is how the banner will appear at the top of your email:

Visit this website for more information.

Kind regards,

Email – September 23 - Complete

- ACE IT (morning of September 23)
- EITU (morning of September 23)
- Infotech (afternoon of September 23)

Dear colleagues,

As you may be aware, since March 2020 Information Security and Enterprise Applications and Solutions Integration have worked to introduce external email notification banners for UTmail+ (Office 365).

This banner will help to protect U of T from hacking and phishing attempts, and will also protect our faculty, staff and students' valuable information. These banners will appear on all emails originating from outside the University of Toronto systems.

To date, we have piloted and rolled this banner out to 1,000 users across all three campuses and it has been positively received. As the final phase of this project, we plan to roll the banner out to all remaining faculty, staff and students on September 30.

Thank you to everyone who participated in our pilot program and provided feedback, and we look forward to further improving cyber security for the U of T community.

Visit this website for more information.

If you have any questions, please open a ticket at https://uoft.me/eeber

Kind regards,
Information Security and Enterprise Applications and Solutions Integration

Student Message – September 24 - complete

- Enrollment Services (social media) - confirmed – sent to registrars
- Student Life (social media/newsletter) - sent
- ACORN Launchpad - Navi and COVID messages are taking precedence
- Quercus? (advised there are very few global messages posted and they need to be reviewed by an executive steering committee – we'll try for this channel) - sent
- A&S (social media/newsletters) - confirmed – social media and newsletter
- UTSC (done) and UTM (done) - confirmed
- Help Desk - confirmed

Twitter:

Starting September 30, you may notice a banner marking all emails originating from outside of U of T. This banner will help to remind you to be cautious when opening external emails and attachments, serving as a warning for hacking and phishing attempts. Learn more

Facebook and ACORN Launchpad:

Starting September 30, you may notice a banner marking all emails originating from outside of U of T. This banner will help to remind you to be cautious when opening external emails and attachments, serving as a warning for hacking and phishing attempts. Messages from legitimate U of T senders will not display this banner. This is one of many U of T initiatives to keep your valuable information secure. Learn more

Quercus:

In an effort to reduce hacking and phishing, starting on September 30, U of T emails will include a banner notifying the recipient when a message originated from outside the University. Learn more

EASI Website Announcement – September 24 - complete

- In the Loop (September 29) - sent
- ITS Website – homepage and banner
  - CISO page – link to info
  - Security Matters website – link to info

Information Security and Enterprise Applications and Solutions Integration are pleased to announce that the new external email notification banners for UTmail+ (Office 365) will be rolled out university wide on September 30.

The banner will help to protect U of T from hacking and phishing attempts, and will also protect faculty, staff and students' valuable information. These banners will appear on all emails originating from outside the University of Toronto.

This is how the banner will appear at the top of an external email:

This project, which started in March 2020, included extensive consultation across all three campuses and has been piloted with close to 1,000 users.

Thank you to everyone who participated in our pilot program and provided feedback. You are helping to keep the U of T safe from hacking and phishing attempts and we look forward to further improving cyber security for the U of T community.

Visit this website for more information.

If you have any questions, please open a ticket at https://uoft.me/eeber

Registrars' Message - Complete

- Registrars' Listserv – complete September 24

Dear Colleagues,

Information Security and Enterprise Applications and Solutions Integration are pleased to announce that the new external email notification banners for UTmail+ (Office 365) will be rolled out university wide on September 30.

As you may be aware, this banner will help to protect U of T from hackers and phishing attempts, and will also protect our faculty, staff and students' valuable information.

These banners will appear on all emails originating from outside the University of Toronto. They will serve as a warning for faculty, staff and students to be cautious when opening external emails and attachments that could be potentially malicious.

This is how the banner will appear at the top of all faculty, staff and students' external emails:

This project, which started in March 2020, included extensive consultation across all three campuses and has been piloted with 1,000 users.

Thank you to everyone who participated in our pilot program and provided feedback. You are helping to keep the U of T safe from hacking and phishing attempts and we look forward to further improving cyber security for the U of T community.

Visit this website for more information.

If you have any questions, please open a ticket at https://uoft.me/eeber

Kind regards,
Information Security and Enterprise Applications and Solutions Integration

Knowledge Base Article - Complete

- Added to Enterprise Service Centre

Email to Infotech with Preview Instructions – Complete

- Sent to Infotech by ITS Ed, Awareness & Culture – October 2

Dear colleagues,

On September 30, Information Technology Services (ITS) introduced an external email banner notification on all emails originating from outside of the University's systems.

The goal of this initiative is to mitigate spoofing and impersonation attempts and protect U of T from hacking and phishing attacks. Beginning in March 2020, we consulted extensively across all three campuses and piloted the banner with close to 1,000 users and made adjustments based on that feedback.

This week a number of questions have been raised regarding the length of the banner and its impact on email list preview features. **ITS is currently reviewing these questions and possible mitigation. In the meantime, here are some resources to address reported preview issues.**

During the pilot, we identified and exempted hundreds of internal senders/systems to ensure that legitimate internal communications would not be affected by the external email banner. Exemption requests can be submitted for specific email sources but not for individual recipients. If you are using on-premises relays or legitimate third-party SaaS apps or newsletter bulk mailers that need to be exempt, please submit a ticket via the Enterprise Service Centre using the following link: https://uoft.me/eeber.

Sincerely,
Information Technology Services