One of the easiest ways to get around an organization's security measures to try to trick someone with E-mail phishing. Think of the havoc caused a few years ago to the Cloquet school system.

Each one of us the last line of defence, and the first to be attacked. IT and FDL needs each one of us to protect our Networks and data. We are a huge target. While we have used KnowBe4 as a security resource we have now added Mimecast, to add an additional layer of security.

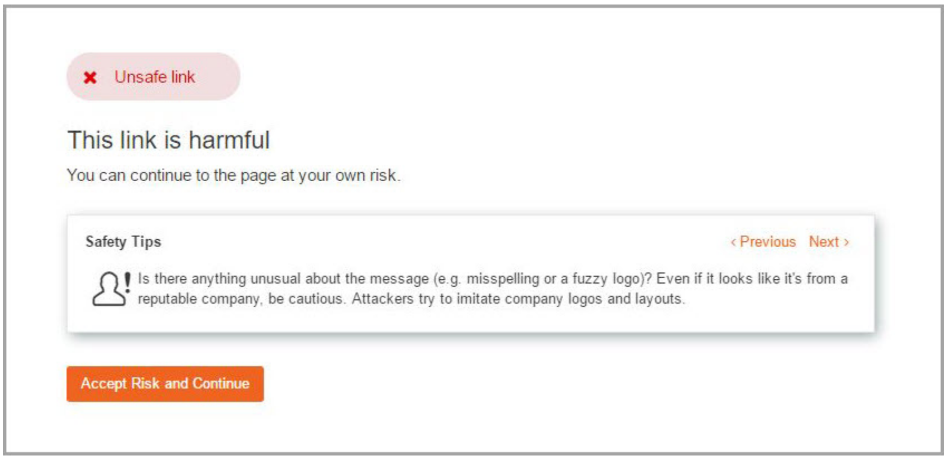
What is Mimecast and how does it relate to user awareness?

As part of our ongoing security focus, we've enabled a new feature in our email security platform from Mimecast that occasionally requires your engagement. The aim is to increase your awareness as a user of potentially harmful content embedded in email, and malicious links found in attachments.

What will I see?

What you'll see depends on the configuration made by your Administrator. For a small percentage of links that you click on in emails, you'll be shown a page with information about the website you're trying to access.

You'll be asked to decide if you're happy to continue to the website, or if you want to change your mind. By prompting you to think before you click, you can help to strengthen our defences. Look out for useful Safety Tips shown throughout these pages, and click the *Previous* or *Next* links to view more.



✖ Unsafe link

This link is harmful

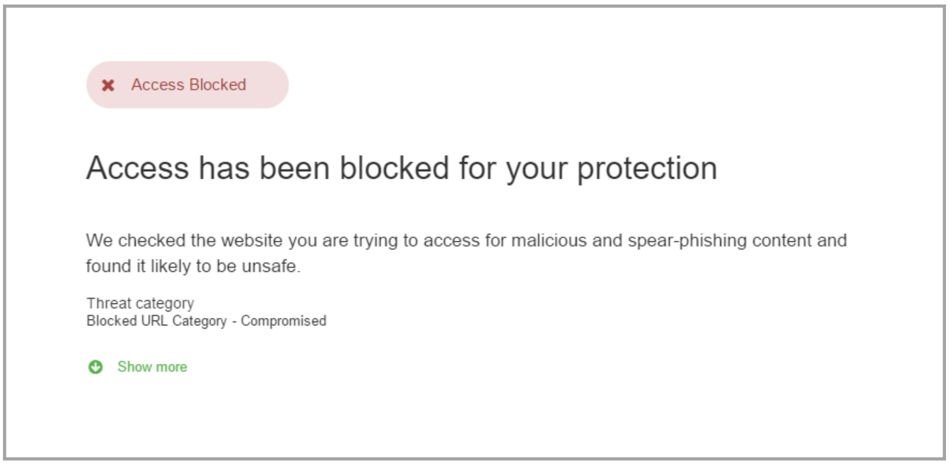
You can continue to the page at your own risk.

Safety Tips

‹ Previous Next ›

Is there anything unusual about the message (e.g. misspelling or a fuzzy logo)? Even if it looks like it's from a reputable company, be cautious. Attackers try to imitate company logos and layouts.

If malicious content is found in the website you're trying to access, you'll be shown the page below. This lets you know that access has been blocked and you'll need to close the browser. Click on the *Show More* link, or contact your Administrator, to find out more information.



✖ Access Blocked

Access has been blocked for your protection

We checked the website you are trying to access for malicious and spear-phishing content and found it likely to be unsafe.

Threat category
Blocked URL Category - Compromised

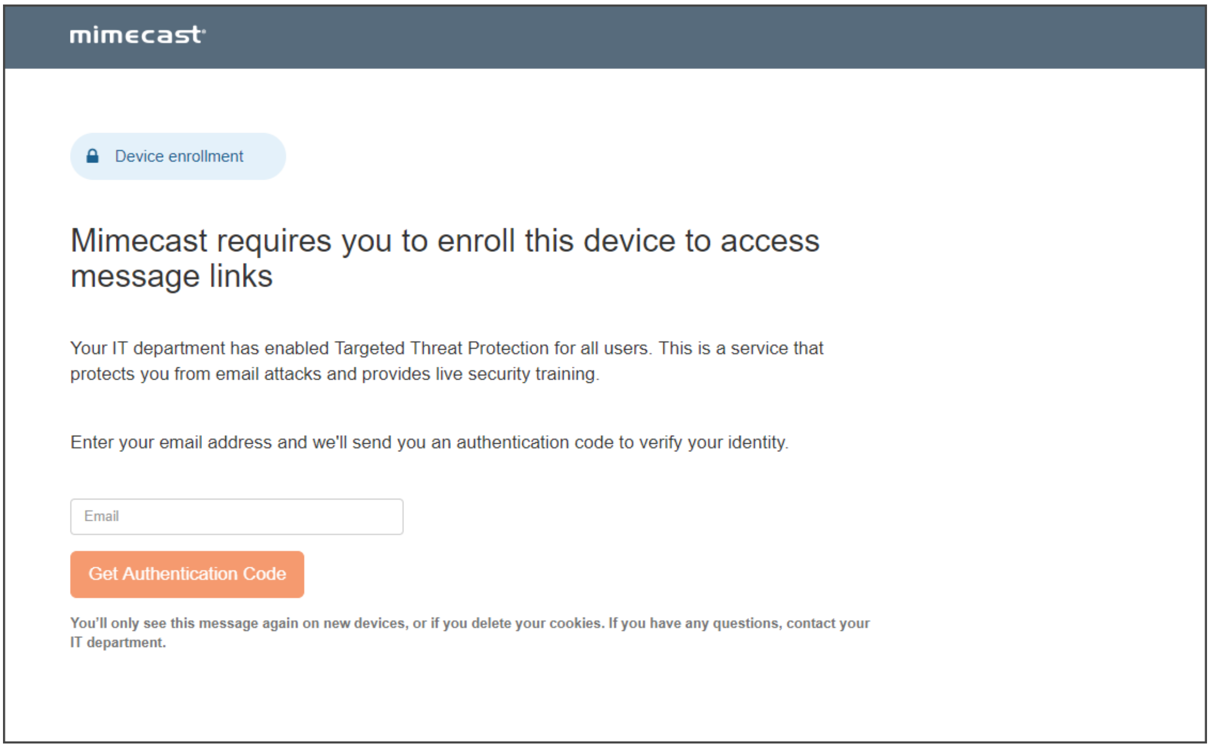
Show more

What do I need to do?

The next time you click a link in an email, or request the release of an original email attachment, you'll be asked to enroll your device to continue.

When prompted in the browser, enter your work email address and click *Get Authentication Code*. You'll receive a one-time code by email to enter into your browser where indicated. If you don't see it quickly check your Junk E-Mail folder.

You'll be asked to enroll once on each device that you use your work email to access (e.g. laptop and mobile). Bear in mind, you'll need to enroll any new devices, or if you delete your browser cookies.



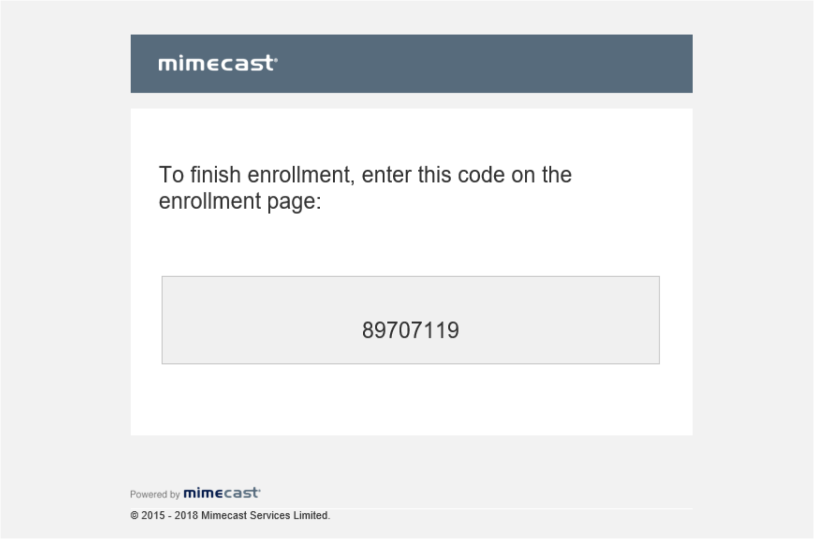
Device enrollment

Mimecast requires you to enroll this device to access message links

Your IT department has enabled Targeted Threat Protection for all users. This is a service that protects you from email attacks and provides live security training.

Enter your email address and we'll send you an authentication code to verify your identity.

You'll only see this message again on new devices, or if you delete your cookies. If you have any questions, contact your IT department.

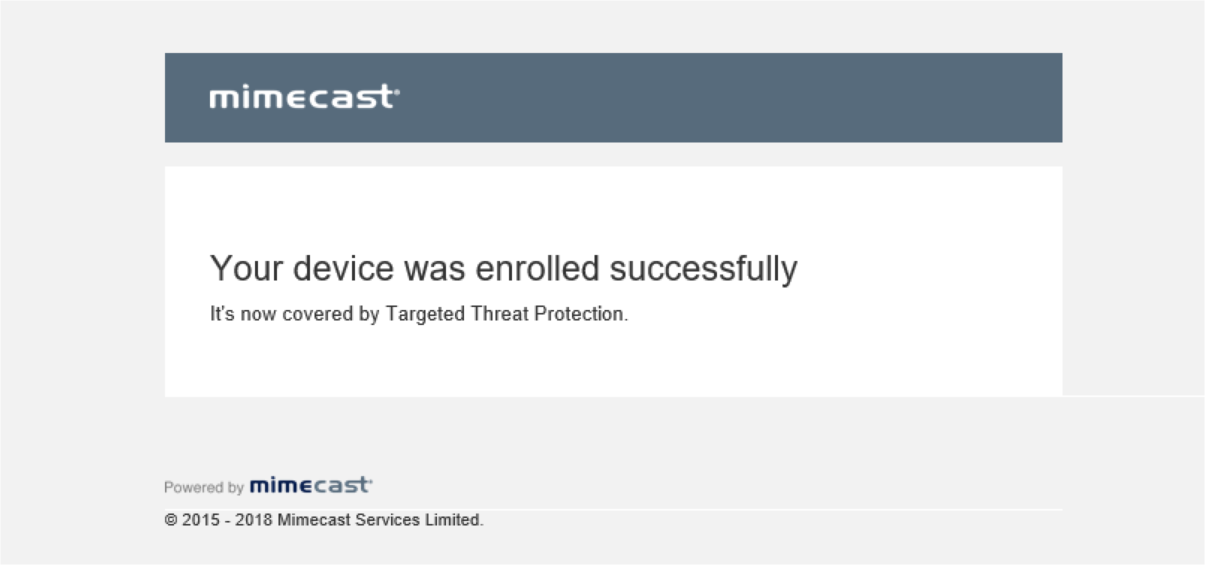


mimecast

To finish enrollment, enter this code on the enrollment page:

89707119

Powered by mimecast



mimecast

Your device was enrolled successfully

It's now covered by Targeted Threat Protection.

Powered by mimecast

If you have any questions or need further help, please contact me at Dianesodengroves@fdlrez.com or call me at 218-878-7476.