TeamLogicIT
Your Technology Advisor

End-User Verification



What Is End-User Verification?

End-User Verification are identity verification techniques that confirm the identity of the respective person. Identity verification, in the context of cybersecurity and access control, refers to the process of confirming and validating the identity of individuals who are trying to access a system, application, or network. The goal is to ensure that only authorized users gain access to specific resources, while unauthorized or malicious actors are prevented from doing so.

Why Does TeamLogic IT Milwaukee Make Use of End-User Verification?

TeamLogic IT Milwaukee has adopted a Zero Trust Policy (ZTP). A ZTP is an approach to cybersecurity that assumes no entity, whether inside or outside the organization, can be trusted by default. This security model requires strict verification of anyone trying to access resources in the network, regardless of their location or the device they are using.

There are several reasons why we have adopted a zero-trust policy

- **Changing Perimeter:** Traditional security models rely on a secure perimeter, assuming that once someone is inside the network, they can be trusted. However, with the rise of remote work, cloud computing, and mobile devices, the concept of a secure perimeter has become less relevant. Zero trust acknowledges that threats can come from both inside and outside the network.

- **Advanced Threats:** Traditional security measures are not always effective against advanced persistent threats and sophisticated cyber-attacks such as AI-induced Voice Phishing Attacks. A ZTP approach helps to mitigate the risk of these threats by continuously verifying and authenticating users.

- **Data Security:** As organizations increasingly store sensitive data in the cloud and allow remote access to their networks, protecting data becomes paramount. ZTP ensures that only authorized users have access to specific data and resources, reducing the risk of data breaches.

- **Mobile Workforce:** With more employees working remotely or using mobile devices to access corporate resources, the traditional model of trusting devices based on their location becomes impractical. Zero trust considers every access attempt as potentially untrusted, regardless of the user's location.

- **Privileged Access:** Zero trust is particularly important for managing privileged access. Even employees with higher levels of access must continuously authenticate and prove their identity, reducing the risk of misuse of privileged credentials.

- **Insider Threats:** While the majority of employees are trustworthy, insider threats can still pose a significant risk. Zero trust helps organizations minimize the potential damage from insider threats by enforcing the principle of least privilege and continuous monitoring.

- **Compliance Requirements:** In many industries, there are regulatory requirements that mandate a high level of security and data protection. Adopting a ZTP can help organizations meet these compliance standards and demonstrate a commitment to securing sensitive information.

What are typical ways to authenticate an identity?

The goal of identity verification is to ensure that the person claiming a particular identity is, indeed, who they say they are. Verification, to be effective, relies on Multi-Factor Authentication (MFA). Here is a list of factors that we rely on:

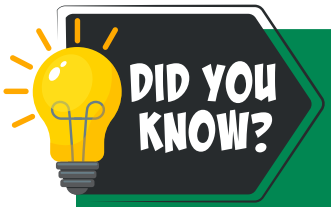
- **Something You Know:** This involves knowledge-based factors such as passwords, PINs, or security questions. Often these are not available at the time of authentication because of forgotten information. They can often be compromised because they are often shared or based upon easily generated information (birth dates, addresses or less.)

- **Something You Have:** This includes possession-based factors such as security tokens, smart cards, or mobile devices. In the case of a mobile device, this usually means the phone number and possession of the device as forms of authentication because you can reference them via a phone call, SMS or an application notification push.

- **Something You Are:** This involves biometric factors like fingerprints, facial recognition, or retina scans. With access to your mobile devices your biometric information authenticated and stored on the device is proof of something that is unique to the end user.

So how does End-User Verification make use of the Authentication Factors listed above?

End-User Verification is a 30-second process and because of our ZTP, it is required on every service desk call from our clients.



Identity threats are up 144% since 2022, dominating alerts and investigations for the third year in a row!

-Annual Threat Report 2024

Table of Contents

SMS 5

Microsoft Authenticator 6

Duo Authenticator 7

Email 8

Landline 11

Client Portal 12

Secure Link 16

Teams 18

SMS Verification

How Is It Done?

If we have a valid mobile phone number on file we can do the End-User Verification via SMS. The published phone number for all Verification requests for TeamLogic IT Milwaukee will come from (262) 800-7992

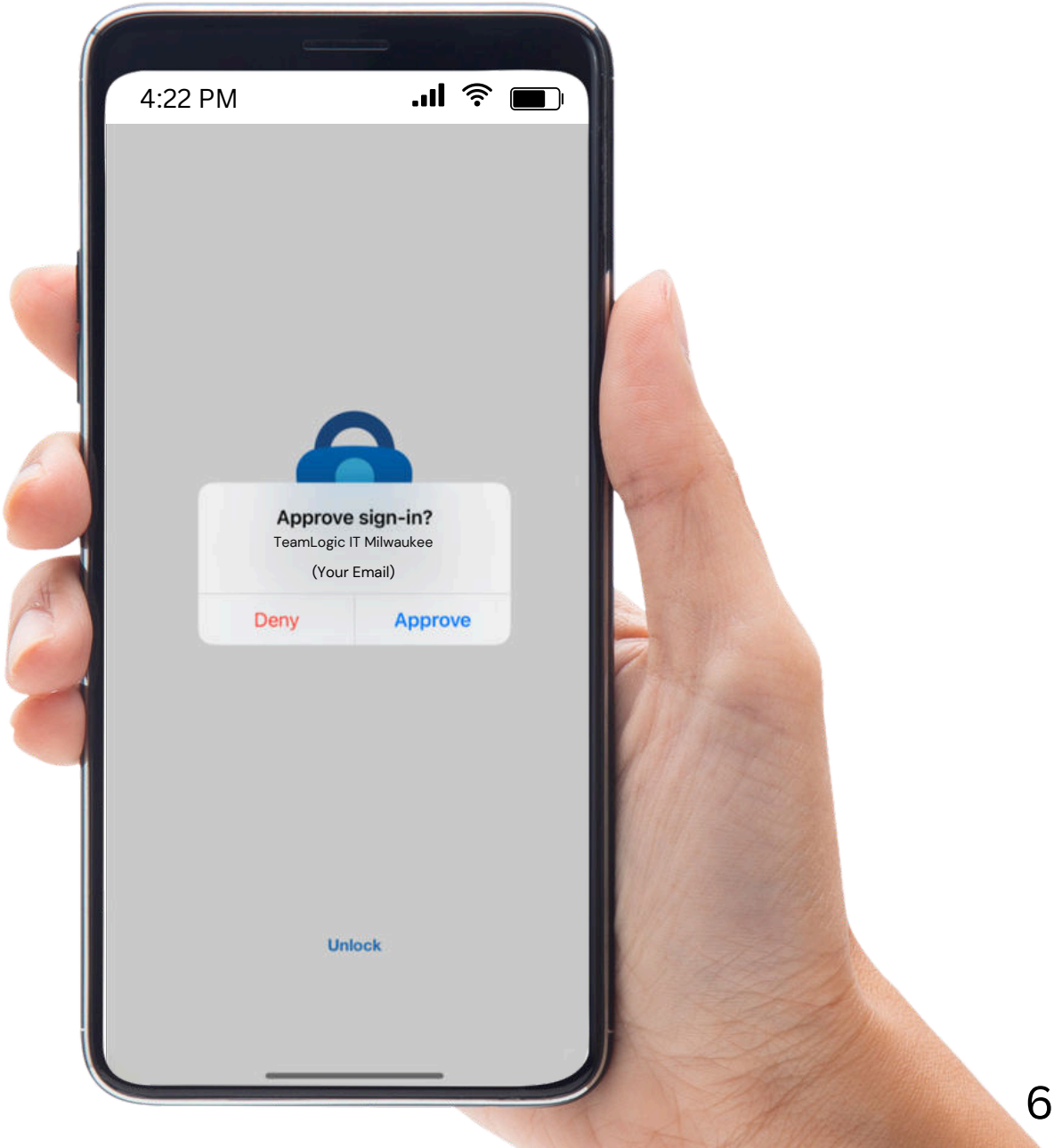
You will receive a six-digit code. Please repeat the six-digit code back to your service desk technician within the specified period of time.



Microsoft Authenticator

How Is It Done?

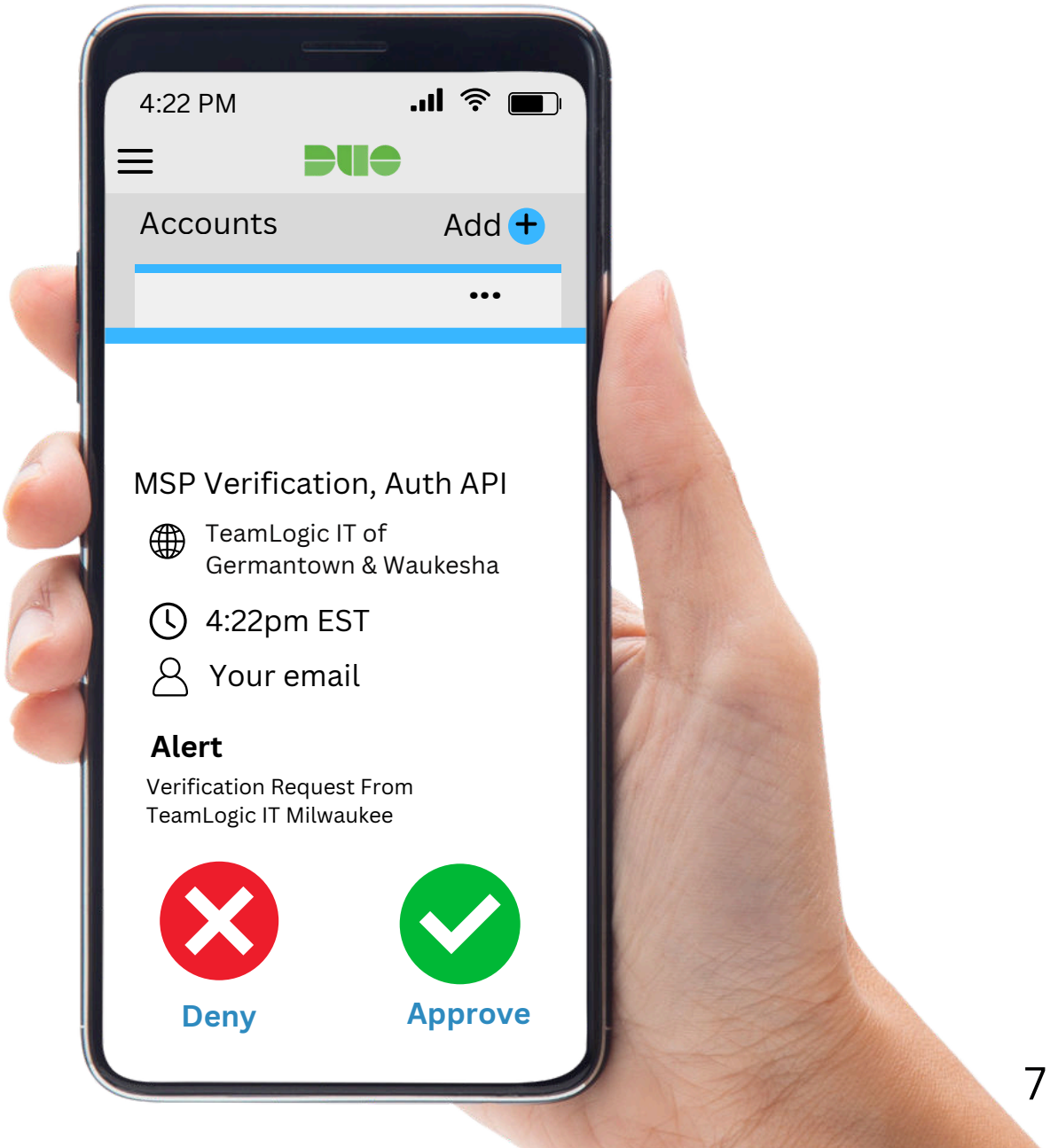
If Microsoft Authenticator has been configured, please go to your Microsoft Authenticator app on your mobile phone and click “Approve”.



DUO Authenticator

How Is It Done?

If Duo has been configured, please go to your Duo Mobile app on your mobile phone and "Approve" the verification push.

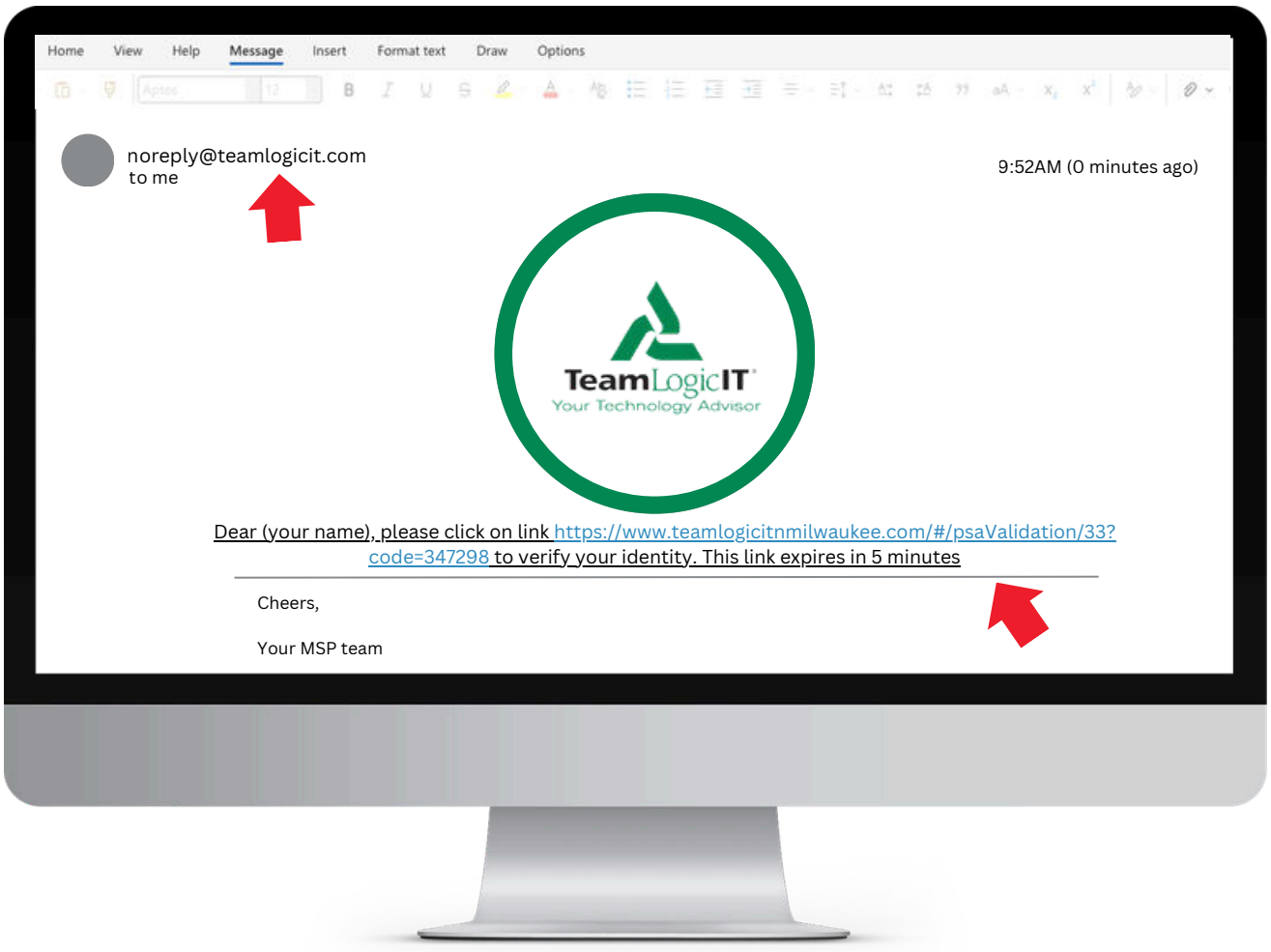


Email

How Is It Done?

If we have a valid email in our system verification, expect that this email will come from noreply@teamlogicit.com

Please click on the link as indicated below within the specified period of time:



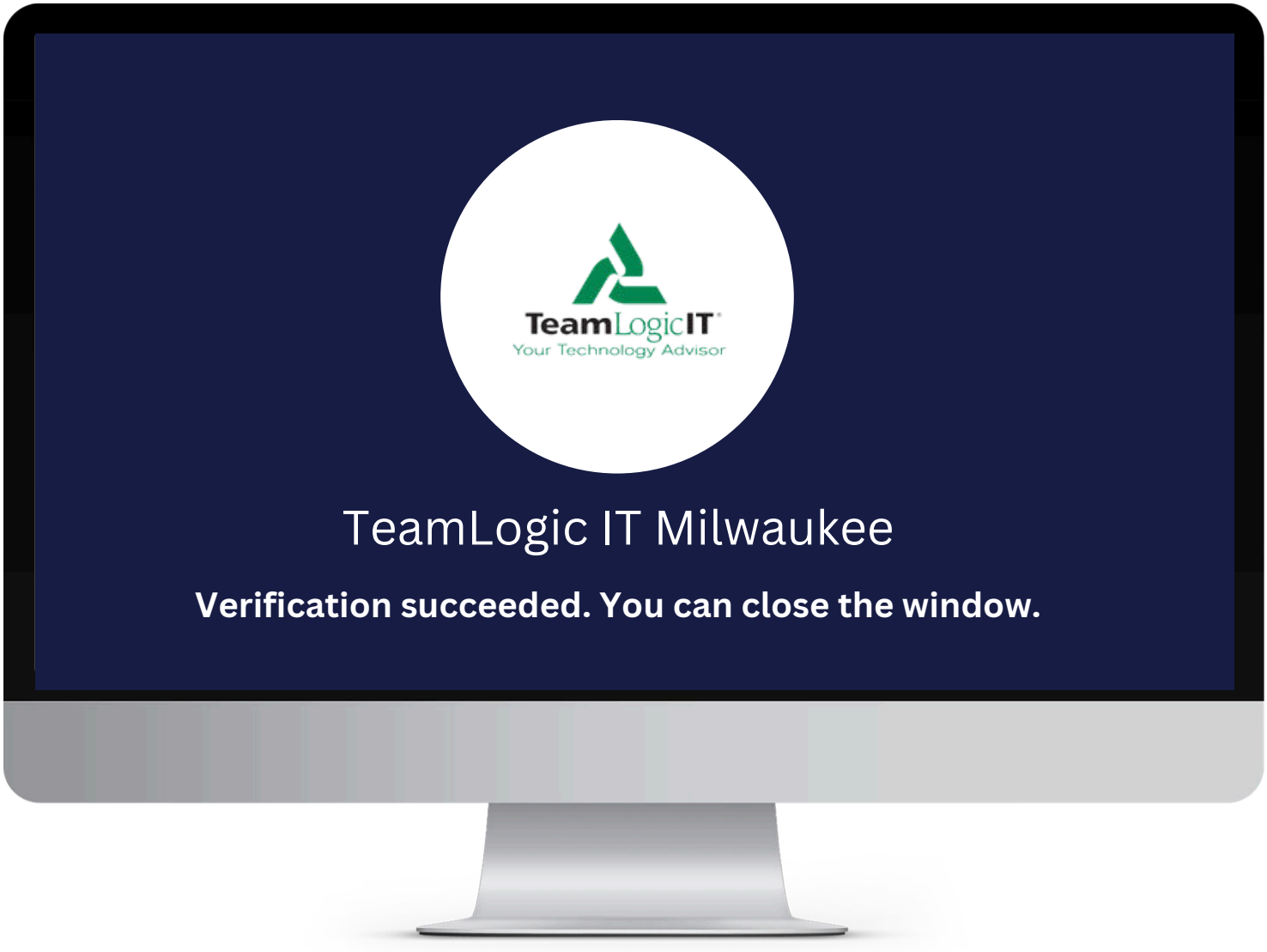
Email

The final step is to click on “Validate”.



Email

If the validation is completed successfully, you will see the following:



Verification is now complete!

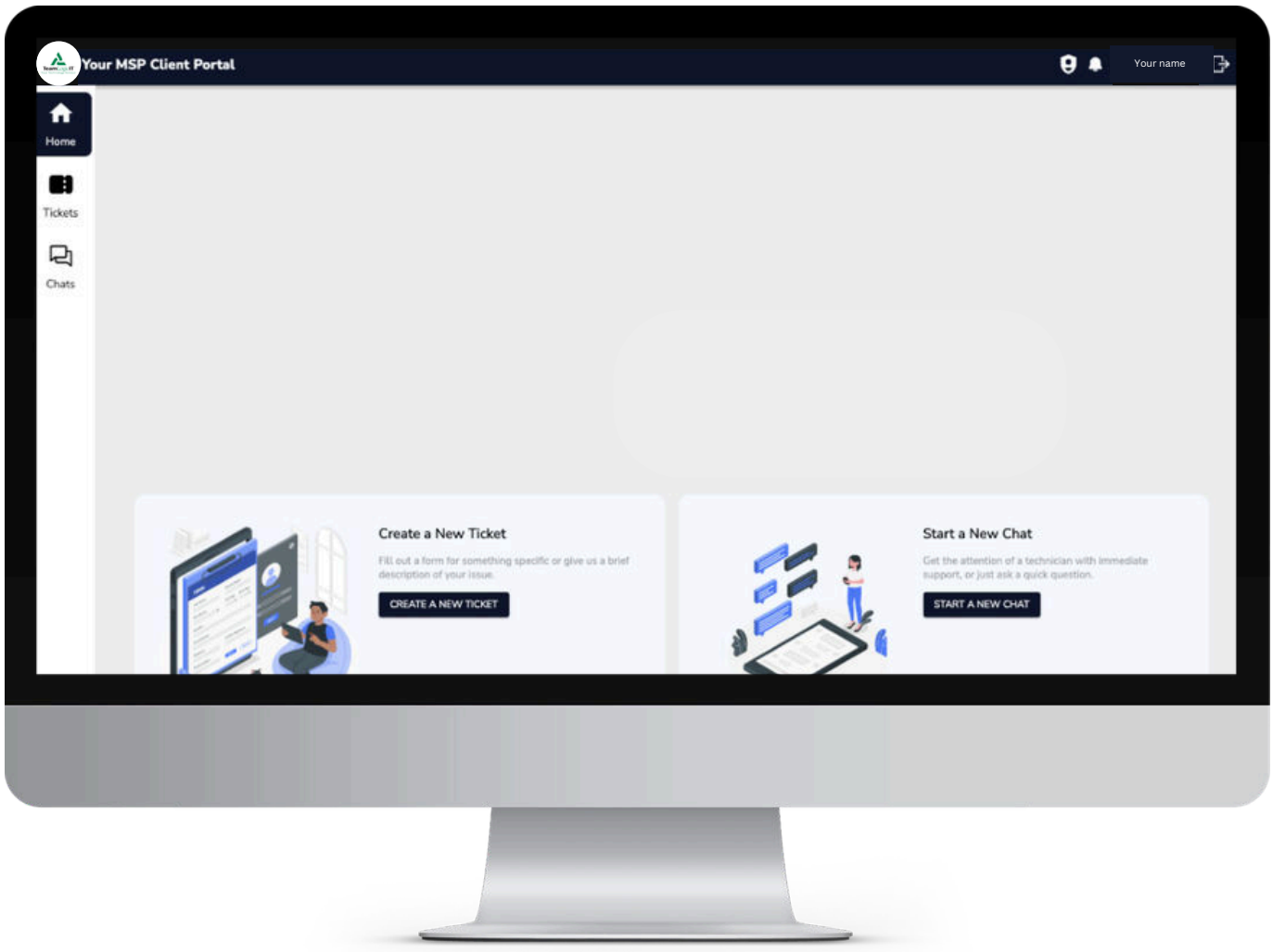
Landline

If no email or mobile phone is available, you can be verified with a voice phone call to the specified landline phone that we may have on file. The automated system will read you a six-digit phone number so be prepared to write this single-use number down. The six-digit will be repeated a second time if you happen to miss the first time. Provide this six-digit code to your service technician. Your technician will confirm the successful completion of the verification.



Client Portal

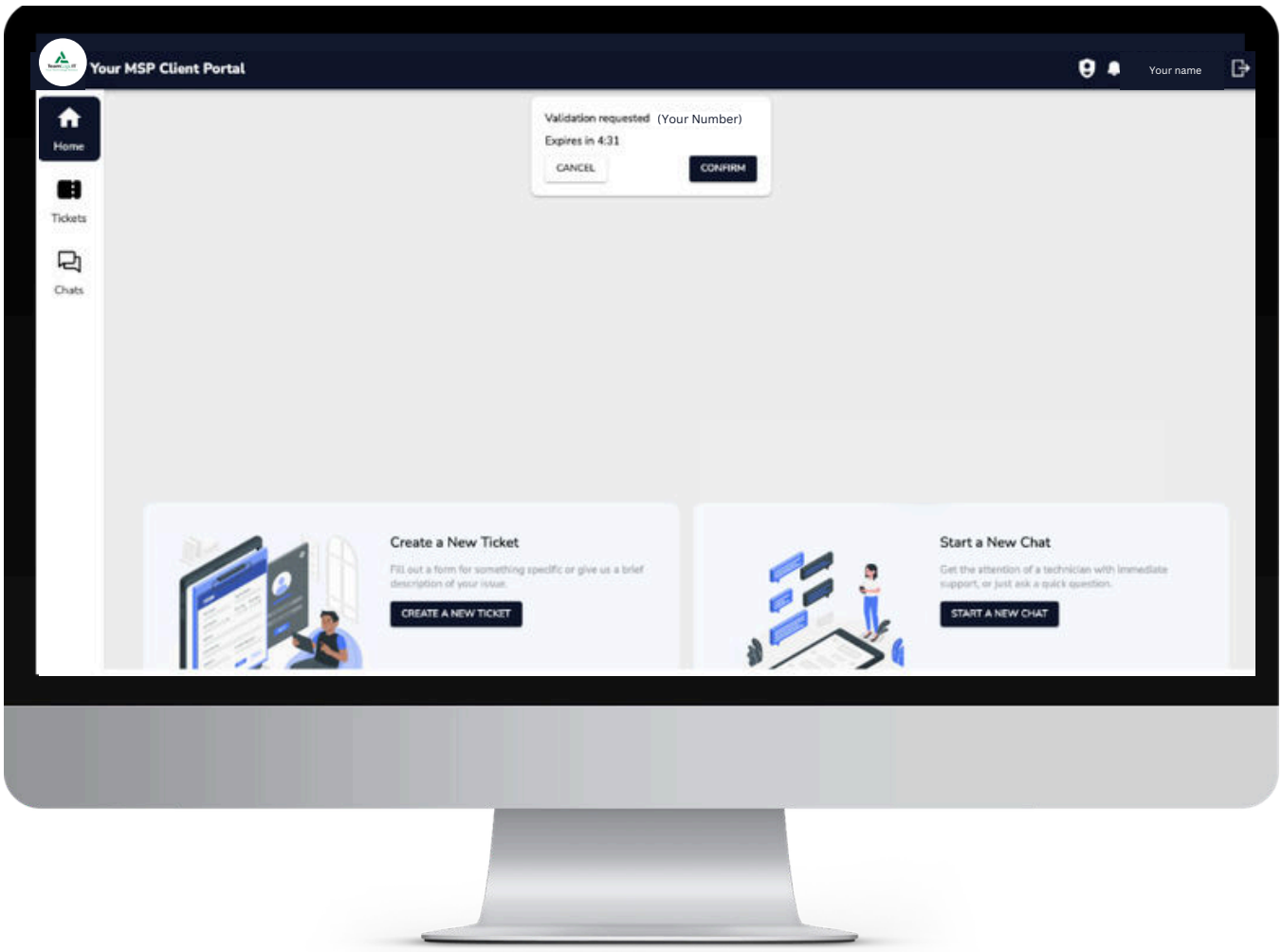
If a client portal has been configured, verification can proceed via the client portal. Please log into the portal with your credential information.



When you are logged in and ready, your service technician will verify you in one of two ways.

Client Portal

First way:
Confirmation from the Client Portal. Click on the "CONFIRM" button before expiration:



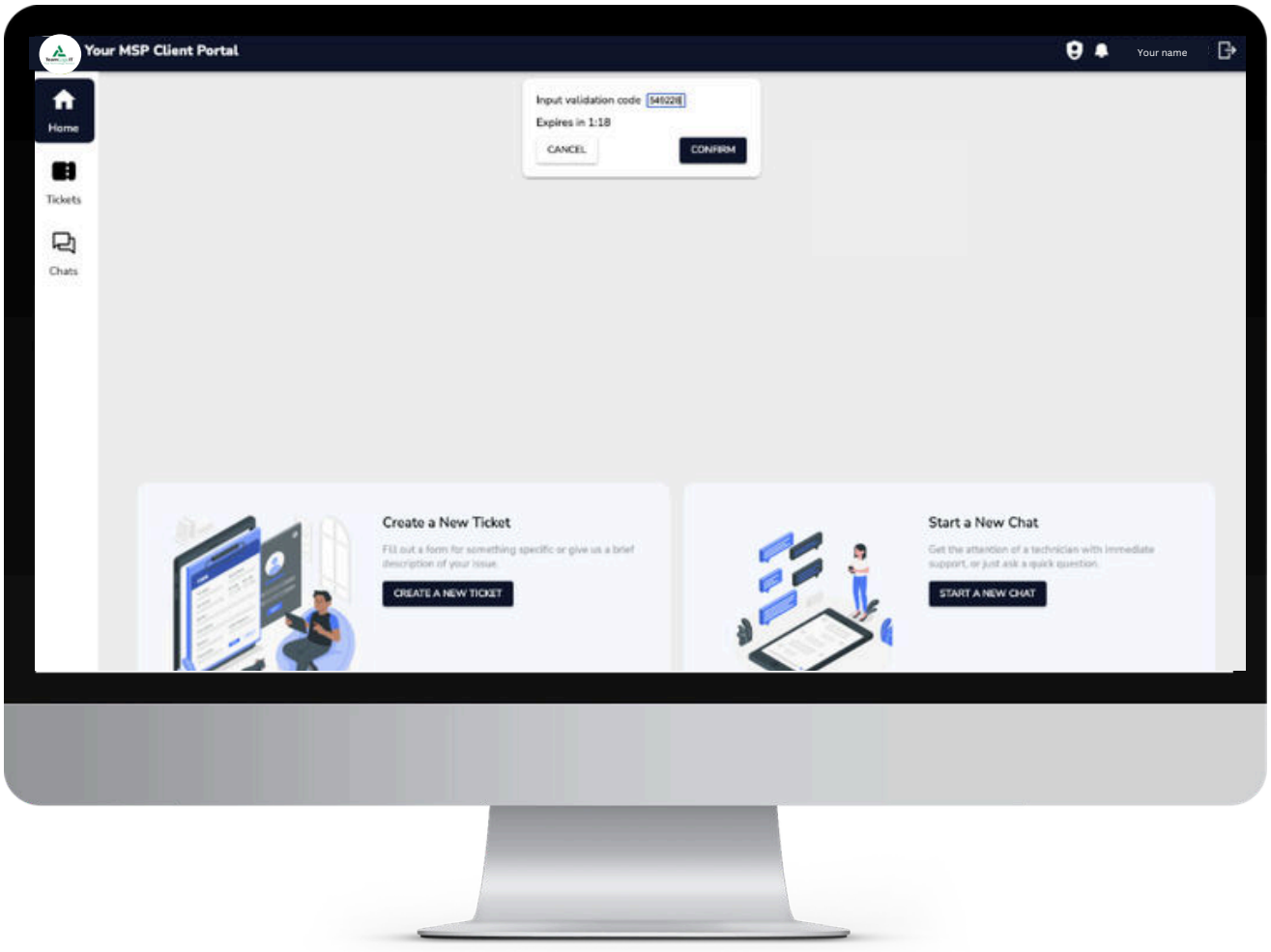
Client Portal

Second way:
Confirmation from the Client Portal with a six-digit code sent via SMS to your mobile phone:



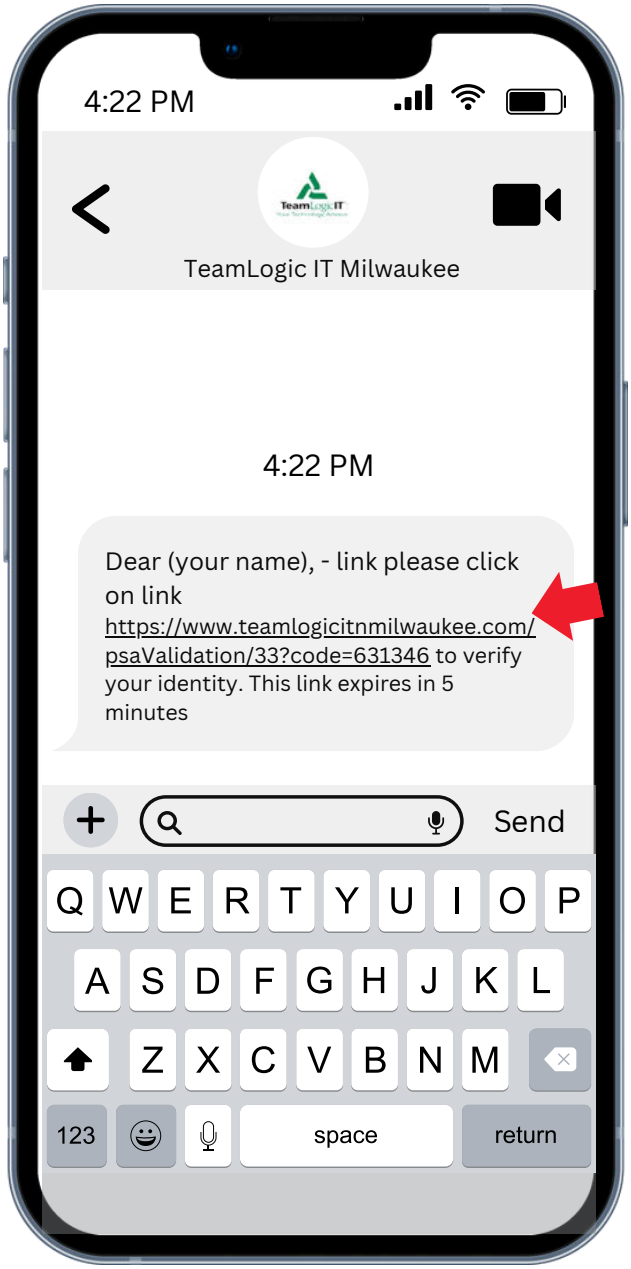
Client Portal

Take the six-digit code that you receive from your mobile phone via SMS to put in the client portal dialog box and click "CONFIRM".



Secure Link

Single-Click Secure Link - when you receive the text via SMS, please click on the validation link as specified below:

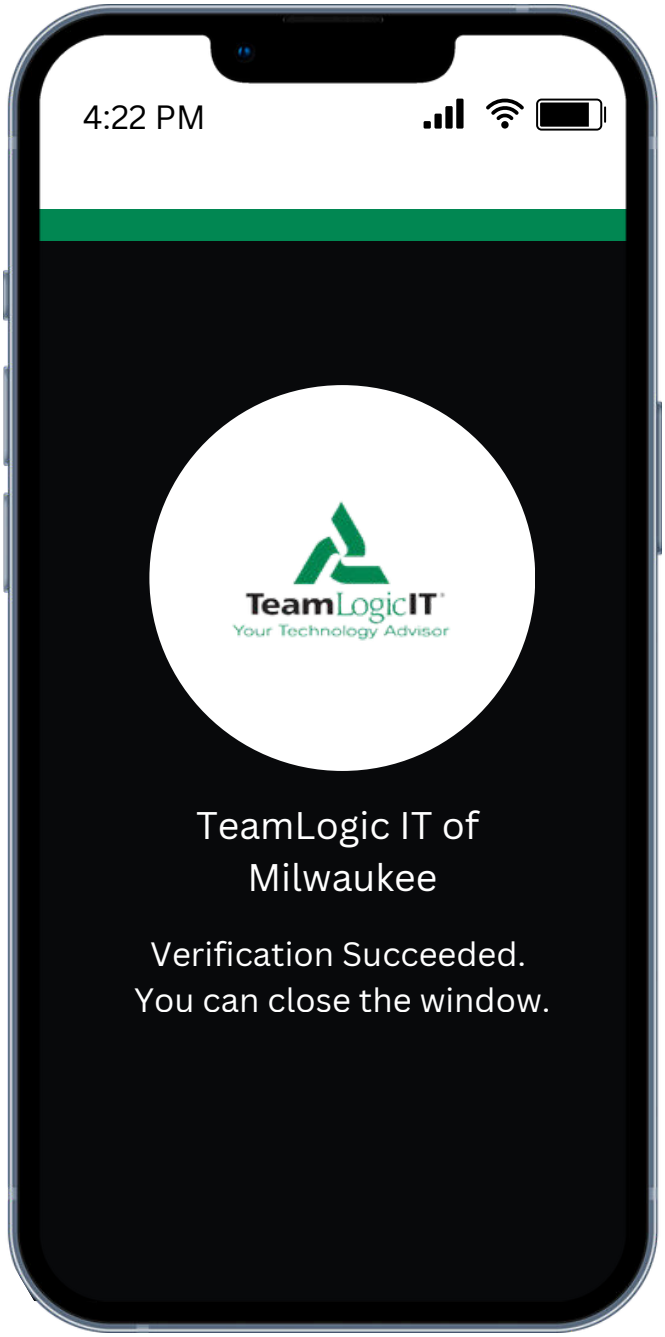




Click on "Validate" to complete the verification process

Secure Link

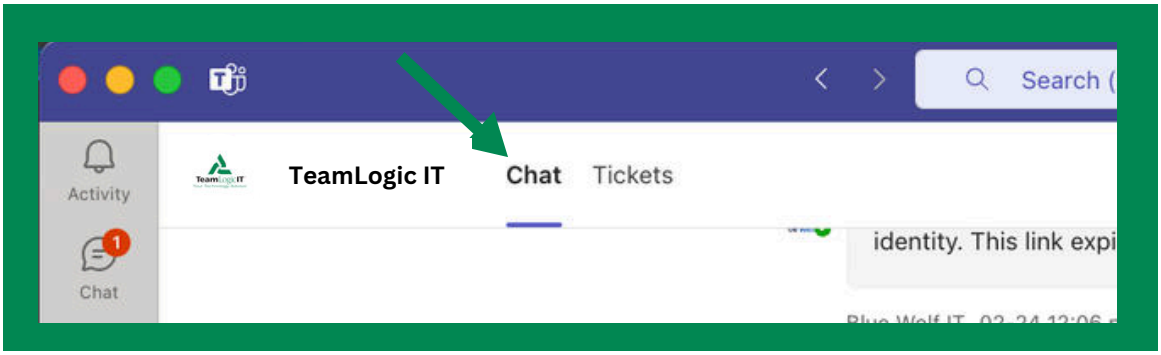
If verification is successful, you will get the following screen. The verification is now complete:

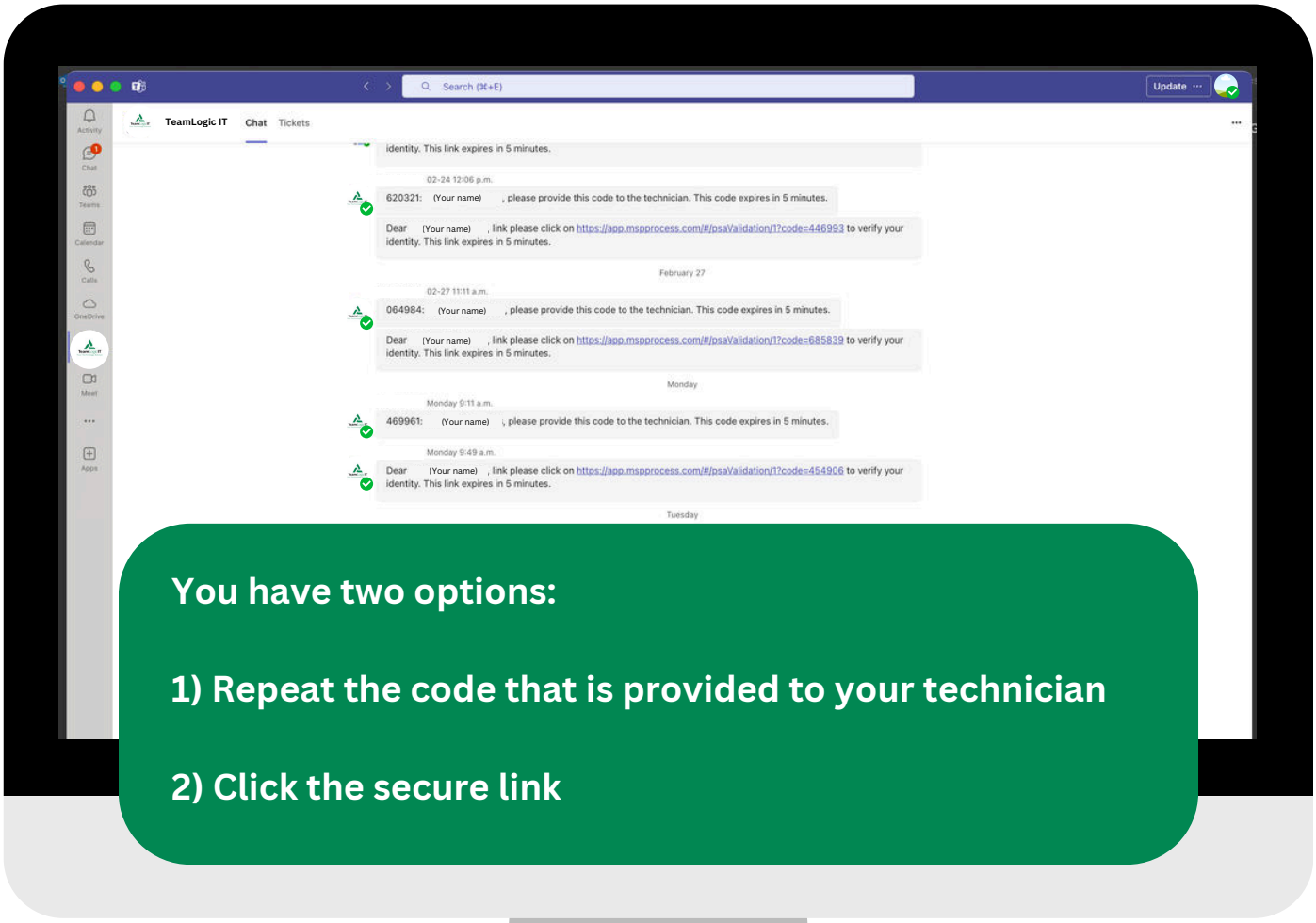


TeamLogicIT
Your Technology Advisor

Teams

Click chat, where all of the verification codes/links will be found.





You have two options:

1) Repeat the code that is provided to your technician

2) Click the secure link

You Are Now Verified!