UMPQUA BANK

Authentication FAQs

What is multi-factor authentication?

Multi-factor authentication is used in the security industry to establish identity by requiring the user to present at least two of three identifying factors:

Knowledge factor — something the user knows, such as a username and password

Possession factor — something the user has, such as a token or mobile phone or tablet that may be used to generate a one-time password

Inherence factor – a unique biological trait, such as a fingerprint or face scan, confirming the identity of the user

What is "evolved authentication" and what are push notifications?

Evolved multi-factor authentication security technology lets you authenticate your online banking transactions in real-time using your mobile device. A simple accept or reject response is given to an authentication request.

We will soon replace the current one-time password (OTP) / secure access code (SAC) system. In the future, when you perform a high-risk online banking transaction, you will receive an interactive pop-up message on your mobile device providing the details of the transaction and requesting you to either accept or reject it. This is called a push notification request. If you do not recognize the transaction or did not initiate it, you can click the reject button displayed in the authentication request and the transaction will not be processed.

Please make sure push notifications are enabled in Settings for your banking application. Push notifications are im¬portant because it gives you full overview and control of all transactions on your account.

Why were one-time passwords / secure access codes replaced?

Umpqua Bank's new authentication method is much more secure because it allows you to accept or reject trans¬actions directly via your mobile phone. You, as the account owner, remain firmly in control of every high-risk transaction because you accept or reject each one before it is processed.

Your response to the authentication request is sent using a separate, mutually encrypted connection directly between your mobile device and the bank. This replaces the need to enter a one-time passcode (OTP) on your computer, where it could be susceptible to phishing and other cyber threats.

What are the risks associated with using one-time passwords / secure access codes?

One-time passwords (OTPs) or Secure Access Codes (SACs) can be intercepted by fraudsters employing cyber-attack techniques referred to as phishing, “man-in-the-middle” or “SIM swap” fraud.

Fraudsters lure unsuspecting users into entering their online banking credentials (username and password) on a site that mimics the real banking site. The fraudster relays the captured information to the legitimate banking site in real-time. This results in the user receiving an OTP on their mobile device. The fraudster then mimics the real bank by asking the user to enter the OTP/SAC on the fraudulent site. Since the unsuspecting user again enters this OTP/ SAC on the fraudulent site, the fraudsters now have everything they need to steal money from the victim’s accounts.

Because Umpqua Bank makes use of the separate, mutually encrypted connection directly between the bank and the user’s mobile device, it does not require any information to be retyped on a website. A fraudulent site never gets all the information required to transact on behalf of the user, which keeps your accounts safe.

How do I manage my devices?

With this new way of authenticating, devices (including browsers) can be added to your account and identified as “trusted.” This creates a trusted environment to increase safety and speed up your authentication steps for future transactions.

To register a trusted device:

First time: Automatic registration takes place. You also have the option to enable your biometrics on your trusted device if the device has this capability.

Adding additional devices: On our website or mobile application, go to Settings > Authenticator Settings > How to link another Mobile App or Another Device. Follow the prompts to identify and register another device or browser to be linked to your account. If the device has the capabilities, you will have the option to activate the biometrics.

Why one-click login?

When transacting on your trusted device, we will verify your identity by authenticating the device or browser that you have registered to your account, meaning you can frictionlessly log in to your profile. You’ll save time and effort.

Will it help when I contact the call center?

Trusted devices are also making call center authentication faster and easier. Instead of asking questions, your agent will now send a push notification to your trusted device to authenticate that you are the account holder. This saves time while ensuring fraudsters do not access your account.

How can I reset my password?

You no longer need to call the call center to change your password or get a new one. Simply change your password yourself on your account. A push notification will be sent to your trusted device to confirm the change. Once you authenticate the request, your password will be updated.

Will this authentication work on my phone or tablet?

The application is available for all devices running iOS (iPhones and iPads), and Android operating systems. If your phone has a color screen and a browser and can run common applications (e.g. Mxit or Facebook), it should be able to support the au¬thentication.

If I perform bundled payments, will I have to authenticate each payment?

When performing multiple or bundled payments, you will receive only one message for authenticating the bundled transac¬tion. The message will contain a figure showing the total value of the bundled transactions and the number of transactions being performed. You will have the choice to either accept or reject the bundled payment.

Will it cost me money to authenticate?

When performing multiple or bundled payments, you will receive only one message for authenticating the bundled transac¬tion. The message will contain a figure showing the total value of the bundled transactions and the number of transactions being performed. You will have the choice to either accept or reject the bundled payment.

Will the authentication work when I travel abroad?

If you travel abroad, the authentication will work wherever you have Wi-Fi internet connectivity. It will also work if you have roaming data connectivity (GPRS, EDGE, 3G, 4G, 5G, etc.). You may incur roaming data charges even though it uses a very small amount of data.

If you have no internet connectivity, your bank will request you to enter an OTP in order to transact. The application has the built-in functionality to generate an OTP on the device when it has no mobile communication.

How long does it take on average for an authentication message to appear?

If you travel abroad, the authentication will work wherever you have Wi-Fi internet connectivity. It will also work if you have roaming data connectivity (GPRS, EDGE, 3G, 4G, 5G, etc.). You may incur roaming data charges even though it uses a very small amount of data.

If you have no internet connectivity, your bank will request you to enter an OTP in order to transact. The application has the built-in functionality to generate an OTP on the device when it has no mobile communication.

What does it mean when a message “times out” on my mobile phone?

A timeout occurs when your response to the authentication request message takes longer than the bank allows. This might be due to the message taking too long to reach your mobile device or if you take longer to respond to the message. For security reasons, your bank sets limits on the length of time you have to respond.

If a timeout happens, click the resend button (this will be implementation-specific) on your online banking screen to send another message. If timeouts occur repeatedly, call us at **(866) 486-7782** or use Go-To live chat from your account dashboard for assistance.

What should I do if I receive an authentication request message when I did not initiate the transaction?

If you receive an authentication request message for a high-risk transaction on your account that you did not initiate, click reject to stop the transaction. Immediately call us at (866) 486-7782 so that we can take action to stop any suspected fraud attempts.

What will this mean for those who share a username and password with others to access accounts?

While we do not recommend that people share User ID's or Passwords, the first user to sign on and go through the trusted device process will receive push notifications. When the other user uses the shared username and password on a non trusted device, they will not receive the push notification. It is highly recommended each user register and use unique credentials.

www.umpquabank.com

(866) 486-7782