

We understand that the security of individuals' personal information is important. Our continued success relies on our ability to maintain a robust security program consistent with the ethics of privacy and confidentiality in the financial services and health care delivery industries.

Security is not a one time event. Good security is not simple. It is our job to understand, select, and deploy a variety of risk mitigation safeguards. We use a complex set of interacting networks, application and operating system safeguards include: Firewalls, Intrusion Detection, Monitoring Alarms, Encryption, ID codes, Passwords, Digital Certificates, Authentication, Secure Messaging, Audits and Security Tests. When software security improvements are available, we promptly apply them as needed. When new threats are discovered, we evaluate and act. We have significant resources dedicated to Privacy, Integrity & Security Compliance Services.

We strive to maintain the highest standards of decency, fairness, and integrity in our operations. On the internet, we take a number of measures to authenticate your identity when you access our services. We also take steps to protect sensitive information as it traverses the internet to and from your desktop. We take steps to make sure all sensitive information is as secure as possible against unauthorized access and use. We also review our security measures periodically. We remain strongly committed to safeguarding customer information.

Authentication

We use different pieces of information, collectively known as access codes, to properly identify and authenticate you before allowing you secure access to sensitive information. The first piece of information is an initial User ID that is created from personal information.

Upon first log in, we engage the user to create strong authentication methods utilizing Multi Factor Authentication (MFA). Through MFA we will present security questions along with a personalized image to the user. This image helps the user ensure that they know they are on the bank's valid site. In addition, MFA will register the computer so that we can validate the user. Through the use of device registration and password requirements, this gives the bank the ability to offer a higher level of security and protection of our customer's data.

For further security, we store your User ID and password on an encrypted database that is isolated from the internet.

Data Traversing the Internet

Our site uses the highest levels of Internet security. We require the use of a secure browser and take full advantage of its features such as data encryption-using Secure Sockets Layer (SSL) protocol, user names, passwords, digital certificates and other industry recognized encryption standards.

Please do not disclose your OptumHealth Bank internet access information to anyone. If you feel your account login information has been compromised or to report known incidents of unauthorized account access, please contact OptumHealth Bank immediately.