First Bank & Trust Company

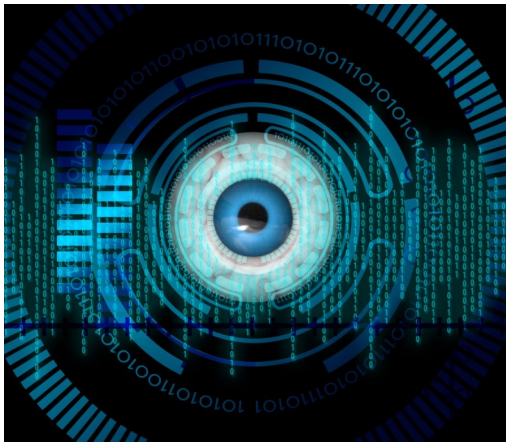
The Bank That Puts You First

Member FDIC

May 2023

Biometrics – Making Security Simple

Overview



Do you hate passwords? Are you tired of constantly logging into new websites or can't remember all of your complex passwords? Frustrated by having to generate new passwords for new accounts or having to change old passwords for existing accounts? We have good news for you. There is a solution called biometrics that helps make cybersecurity easier for you. Below we explain what biometrics are, how they make your life simpler and why you will start seeing more of them.

First, Why Password?

Passwords are part of something called authentication, the process of proving who you are. There have typically been two things you can provide to prove your identity: something you know (like your passwords) and something you have (like an ATM card or your mobile device). Traditionally authentication has been done with passwords. Passwords were first adopted as it was one of the easiest authentication solutions to deploy. However, over the years our lives have become far more complicated with far more accounts than anyone ever expected. It is quite common for a person to have over 100 passwords in their work and personal life.

In addition, cyber attackers have become quite good at guessing, stealing or cracking passwords. This is why you see so many rules about passwords, such as making them long (so they are hard to guess) and using a unique password for every account (so if one of your accounts is hacked, your other accounts are still safe). The problem with all of the password requirements is they make being cybersecure more difficult. Password managers dramatically help as they securely remember all of your passwords and log you into websites for you, but is there a better way? This is where biometrics can help by providing a third thing to prove your identity–something you are.

Biometrics

Like passwords, biometrics are another way to prove who you are. The difference is instead of having to remember something (like your passwords) you use an element of who you are to prove your identity, such as using your fingerprint to gain access to your phone. Biometrics are much simpler as you don't have to remember or type anything, you just authenticate using who you are. There are many different types of biometric such as your voice, how you walk, or your iris prints. However, fingerprints and facial recognition are the two most common, especially for mobile devices. While biometrics have a tremendous number of advantages, they also have some disadvantages, one of the biggest being if your fingerprint or face is copied by cyber attackers, you cannot change them.

Passkeys

Over the coming months and years, you should start seeing biometrics replacing passwords with a new technology called Passkeys. This technology is being adopted by Microsoft, Apple and Google and you should soon see it being adopted at more and more websites over time. Passkeys replace passwords by allowing you to prove who you are by simply using biometrics combined with your mobile device. When you create an account at a website (such as Google or Apple) instead of creating a password you register your mobile device. Moving forward you log into that website by authenticating with your mobile device using biometrics, such as your fingerprint or facial recognition. The website trusts your mobile device, and your mobile device confirms it's you using biometrics. In addition, your biometric data

Continued on page 2

Member FDIC

EQUAL HOUSING LENDER

Virginia Bank Locations
Abingdon, Virginia, East
276-628-3838
Abingdon, Virginia, West
276-628-9558
Blacksburg, Virginia -
540-951-1656
Bridgewater, Virginia
540-266-0003
Bristol, Virginia, East
276-466-9222
Bristol, Virginia, West
276-669-1122
Christiansburg, Virginia
540-260-9060
Fairlawn, Virginia
540-633-3793
Hanover, Virginia
804-550-5700
Harrisonburg, Virginia
540-434-0671
Lebanon, Virginia East
276-889-3401
Lebanon, Virginia West
276-889-4622
Lynchburg Virginia
434-455-0888
Norton, Virginia
276-679-7401
Staunton, Virginia
540-885-8000
Verona, Virginia
540-248-7700
Waynesboro, Virginia
540-943-5020
Wise, Virginia
276-328-3439
Woodstock, Virginia
540-459-7228
Wytheville, Virginia
276-228-1125
Operations Center
276-623-2265

Tennessee Bank Locations
Bristol, Tennessee
Volunteer Pkwy
423-652-2022
Gray, Tennessee
423-467-9966
Johnson City Tennessee
423-975-9900
Kingsport, Tennessee
423-246-3700

First Bank & Trust Loan Production Offices
Bedford, Virginia
540-583-5458
Daleville, Virginia
540-966-7006
Hanover, Virginia
804-550-5700
Lynchburg, Virginia
434-509-0444
Mount Airy, North Carolina
743-212-2013
Red Oak, North Carolina
252-220-4208
Roanoke, Virginia
540-774-0269
Rocky Mount, Virginia
540-484-0338
Winchester, Virginia
540-545-8110
Wytheville Annex

First Bank & Trust Mortgage Lending Division
Bristol, Virginia
276 -644-9900

(fingerprint or face) is not sent to any website. Instead, your biometrics is securely stored locally on your device. It's just used to unlock the "Passkey", a unique key, created for each site, which your device sends to the site while protecting your biometric data. While no solution is perfect, biometrics and solutions like Passkeys can help keep you secure while simplifying security.

Sources:
Article: *Dr. Johannes Ulrich, Dean of Research for the SANS Technology Institute college, SANS OUCH! Newsletter, January 4, 2023*
Images: *Gerd Altmann, Public Domain Pictures*

The Use of Biometrics Technology in Everyday Life

Biometrics has become a buzzword in the last few years, gradually becoming one of the most important industries in the digital universe. According to MarketsandMarkets, the global biometric technology market is expected to grow from USD 42.9 billion in 2022 to USD 82.2 billion by 2027. Increasing advancements in biometric technology across various sectors, rising demand for authentication and identification solutions, and security surveillance solutions are the primary factors driving the market growth.

But what makes this technology so important? How does it affect the world as we know it? While most people believe biometric technology is jeopardizing personal security and privacy, the fact remains that it brings substantial benefits to our everyday lives for a few reasons:

Biometrics ensures accuracy.

- The system eliminates the vast majority of safety threats.
- Many biometrics solutions are cost-effective.
- It is easy to use.
- User acceptance is increasing

Here are some common uses for biometrics in everyday life:

Airport Security

Biometric systems have been in use at airport for quite some time. As facilitating passengers' passage through airports is a universal priority, some of the world's largest airports have utilized biometric technology to verify passenger identities for many years, and this practice is gradually spreading.

Law Enforcement

Biometrics is widely used across law enforcement, with agencies such as the FBI and Interpol utilizing biometrics in criminal investigations. M2SYS technology has been working with law enforcement agencies worldwide to deliver biometric solutions to identify criminals in the last two decades. A collection of solutions designed to meet government law enforcement agency identification & data management requirements while delivering fast, secure, and reliable results.

School

Many developing countries have already implemented biometric technology on school premises. It is also a growing technology that other countries follow to implement in the education sector. Authorities of educational institutes are implementing biometric identification for several reasons. These reasons are mainly segregated into two — one is for internal control, and the other to ensure safety and security. In recent years, many unwanted incidents, like terrorist attacks, vandalism, and mass shootings, have been taking place in educational institutions worldwide, influencing us to rethink security measures in schools, colleges, and universities.

Hospitals

In modern hospitals and clinics, biometric identification is utilized for secure, reliable access to patient's medical records and personal information. The patient's medical history is protected, and no duplicate is created, greatly assisting the healthcare industry. In addition to saving the lives of unconscious patients, quick identification with biometric technology lets hospitals make better treatment decisions based on patient's medical histories.

Blood Collection

Blood is collected from donors and stored in blood banks. However, there are still significant dangers associated with receiving blood from professional or proxy donors. Instead of saving lives, blood donations could take one if the donor isn't adequately screened. Because of this, blood banks now use biometric identification technology to enroll donors, keep track of their medical history, and screen out unqualified donors.

Summary

Whether we like it or not, biometrics are becoming a fundamental part of our daily lives. Many of us will rely on biometrics as a standard method of gaining access to the many products and services we use daily as technology advances. M2SYS aims to simplify the whole process, so anyone can access it without breaking the bank. All you need is to contact us. We'll give you the whole "Turnkey" solution according to your requirement.

Source: *Stanly Palma, M2SYS*

Top Tips for Spotting Deepfakes Online

Deepfakes—digital manipulations of media that use artificial intelligence to create realistic, altered images or videos—can be used to create seemingly genuine footage of people saying or doing things that they never actually said or did.

Researchers, visual effects specialists, amateur enthusiasts, and even porn producers are all creating deepfakes now. It's also possible that political parties and governments are producing deepfakes to try to discredit extremist groups or opponents.

While deepfakes have the potential to revolutionize certain industries, they also pose significant risks to society. Nefarious parties can easily spread misinformation and propaganda using deepfake technology, potentially leading to harmful consequences.

It's important that we, as internet users, build our digital literacy skills so we can successfully navigate our online world—in everyday life, in education, and at work.

A big part of digital literacy is learning how to think critically about what we see and hear online. One important digital literacy skill is being able to identify and debunk deepfake content to protect ourselves and others from being misled.

How to spot a deepfake

If you'd like to see some very convincing deepfake videos, you can look at this Morgan Freeman video from Dutch YouTube creator Diep Nep, or check out the series of fake Tom Cruise videos from visual and AI effects artist Chris Umé.

There are positive uses for deepfake technology—like creating digital voices for people, or updating film footage instead of reshooting—however, as the tools get more sophisticated, the potential for malicious use of deepfakes is concerning.

For example, if malicious actors were to present a deepfake of a world leader as a genuine communication, it could pose a threat to global security. Given the speed at which "fake news" can spread around the world, there is a real threat that people or organizations could use deepfakes to manipulate public opinion and deceive others into believing they are authentic representations.

Here are 4 things to look for if you suspect you might be looking at a deepfake:

Unnatural facial or eye movements

It's difficult for deepfake producers to accurately reproduce eye or facial movements and imitate the ways humans blink. When examining questionable videos, look for strange eye movements or a face that doesn't display normal-looking emotions that match what's being said.

Mismatches in lighting and color

Does the skin tone of the person in the video look odd? Is the lighting peculiar, or are there strangely-positioned shadows on the person's face? Take note of discrepancies in the video, and if possible, compare the lighting and color to an original reference photo or video.

Poor audio quality

Producers of deepfake videos often focus more on visuals than on sounds, so watch out for poor lip-syncing, strange word pronunciation, robotic-sounding voices, or digital background noise.

Problems with body movement

If the person in the video appears distorted when they turn to the side or move their head—or if their movements look disconnected or choppy from one frame to the next—you might be looking at a deepfake video.

Awkward posture

Deepfake technology often concentrates on facial features rather than on the entire body, so it can be easy to detect body position and posture anomalies.

If the person's body shape doesn't look natural in the video, or if their body or head is positioned inconsistently or awkwardly, you could be looking at a deepfake video.

Deepfakes are not a passing trend and will be a continuing presence online. As deepfake technology continues to advance, it will become even more important for audiences to be vigilant in identifying fake videos so they don't fall victim to manipulation.

Sources: Article: ***Bernard Marr, Readers Digest, January 27, 2023***
Image: ***Gerd Altmann, Public Domain Pictures***