SMART EYE TECHNOLOGY®
TECHNOLOGY FOR YOUR EYES ONLY®

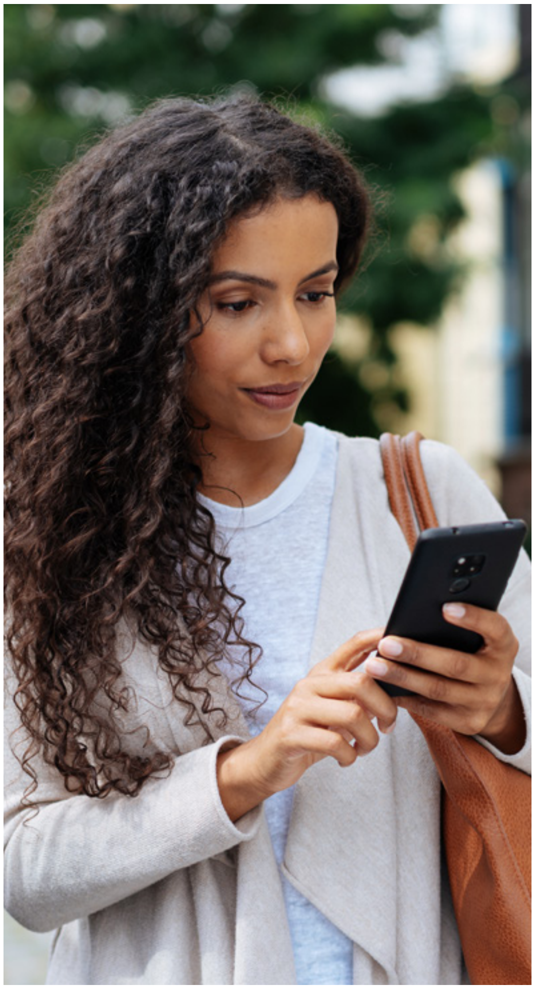
How Biometric Technology is Winning the Battle to Safeguard Document Privacy and Data Security

I. The State of Cybersecurity

Today's organizations face an incredibly broad range of cybersecurity threats.

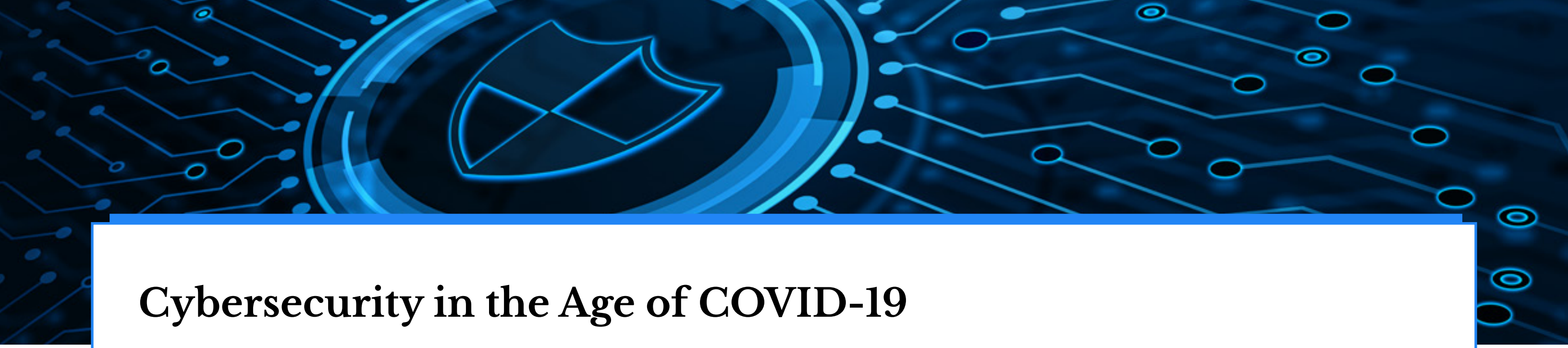
From phishing scams and identity theft to ransomware attacks and cyberfraud, hackers are constantly deploying new strategies to gain access to valuable data.

The fallout from a data breach can bring even a successful company to the brink of ruin. In addition to the time and effort required to address the incident, breaches can also result in lost revenue due to downtime, missed opportunities, regulatory fines, and long-term brand damage. In 2020, these factors combined to bring the average cost of a data breach up to $3.86 million, a 10% increase over the previous five years.



Cybercrime: By the Numbers

- A hacking attempt takes place every **39 seconds**
- **1 in 3 Americans** are affected by a hack each year
- **43% of cyberattacks** target small businesses
- **38% of malicious file extensions** use Microsoft Office document formats
- **41% of companies have no access restrictions** on more than 1,000 files
- **30% of phishing emails** are opened
- **80% of breaches** are tied to passwords
- **29% of breaches** involve the use of stolen credentials
- **52% of visual hacking attempts** captured data from computer screens
- **57% of middle-market businesses** have received fraudulent invoices



Cybersecurity in the Age of COVID-19

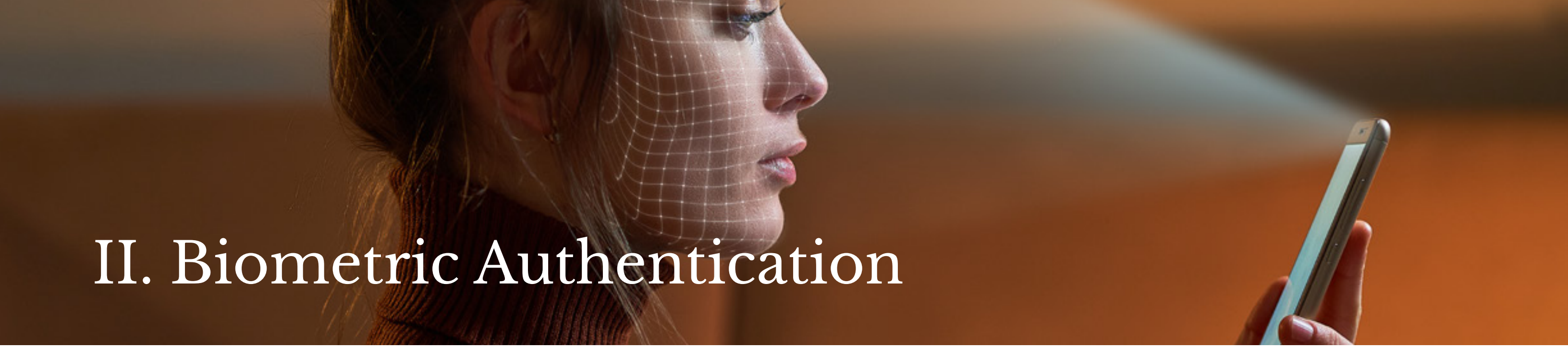
The COVID-19 pandemic forced many companies to transition into remote work situations. Unfortunately, many of them were not prepared to deal with the cybersecurity risks that come with working remotely. Seizing on vulnerabilities like unsecured home networks, cybercriminals have launched a variety of attacks, resulting in a 273% increase in data breaches in the first quarter of 2020.

Email quickly proved to be a uniquely vulnerable component of the remote office. Phishing scams seeking to exploit uncertainty and fear surrounding the pandemic used email messages purporting to be from trusted government sources, well-intended charities, and even corporate CEOs to gain access credentials. After obtaining passwords and log-in information, hackers can penetrate networks to access secure data and documents stored on the company's network.

> cybercriminals have launched a variety of attacks, resulting in a **273% increase in data breaches in the first quarter of 2020.**

The increased threat of credential theft in the remote workplace has made it clear that new forms of document security will be necessary. Organizations need to know that their confidential documents, invoices, and records cannot be accessed by unauthorized users. With so many unusual transactions taking place during the pandemic (such as expedited orders, unexpected refunds, and hastily arranged deals), fraud attempts that might normally raise an alarm could go unnoticed. These trends will surely continue in the post-pandemic environment. With innovative, enhanced forms of document security in place, businesses can block malicious hackers from gaining access to essential data and network systems.

Just because employees are working from home doesn't mean their entire household should have access to essential business information. Without a strong security solution in place to prevent outside threats and visual hacking efforts, sensitive financial data, and proprietary assets might be easily exposed to family members, friends, neighbors, or home contractors. Visual hacking, which can consist of nothing more than a quick glance at an open screen, is successful at capturing sensitive information 91% of the time and goes unnoticed in 68% of cases.

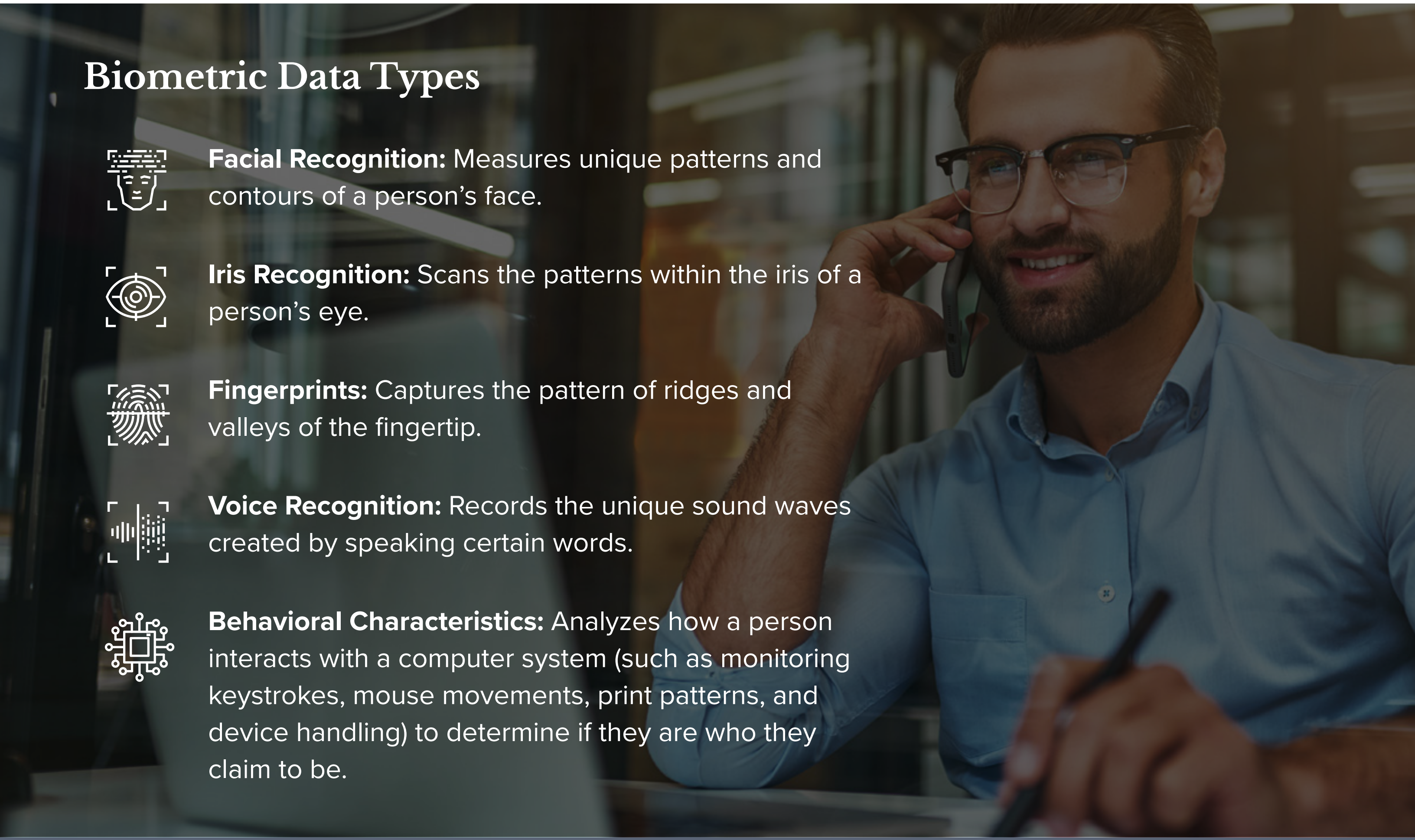


II. Biometric Authentication

For many years, online security measures relied on password authentication out of necessity. Recent advancements in biometrics technology, however, have sparked a revolution in identity verification. Smartphones have played a key role in promoting biometric recognition systems as a safe and secure form of authentication.

How Biometrics Work

The basic concept behind biometric authentication is quite simple. Every person possesses unique physical characteristics and behavioral identifiers. Many of these traits, such as the distinctive patterns of the iris, the contours of the face, or the sound waves created by regular speech, can be measured and stored as biometric data. Once these identities are on file, they can be compared with newly scanned biometric information to see if there is a match.



Biometric Data Types

Facial Recognition: Measures unique patterns and contours of a person's face.

Iris Recognition: Scans the patterns within the iris of a person's eye.

Fingerprints: Captures the pattern of ridges and valleys of the fingertip.

Voice Recognition: Records the unique sound waves created by speaking certain words.

Behavioral Characteristics: Analyzes how a person interacts with a computer system (such as monitoring keystrokes, mouse movements, print patterns, and device handling) to determine if they are who they claim to be.

Any biometric scanning system consists of three essential components:

Biometric Sensor: Typically a camera or a touch sensor, this is the primary input for entering biometric information when seeking to authenticate identity.

Computer Database: In order to verify biometric data, the scan must be checked against existing biometric scans to ensure there is a match. This information must be stored in a secure, encrypted database to prevent biometric data from falling into the wrong hands.

Biometric Software: Using an app or security program, biometric software connects the sensor to the database quickly and securely. A good biometric software solution needs to have strong encryption protocols to ensure that personally identifiable information is not stolen or misused.

Today's devices are uniquely well-suited for deploying biometric authentication systems.

The latest generations of smartphones and laptops are equipped with the sensitive touch sensors and high-resolution cameras necessary to capture biometric data accurately.

Thanks to sophisticated apps, that data can be securely stored in the cloud and for later verification.

III. Why Biometrics Are Becoming the “New Normal” for Authentication

Biometric verification offers a number of advantages over passwords.

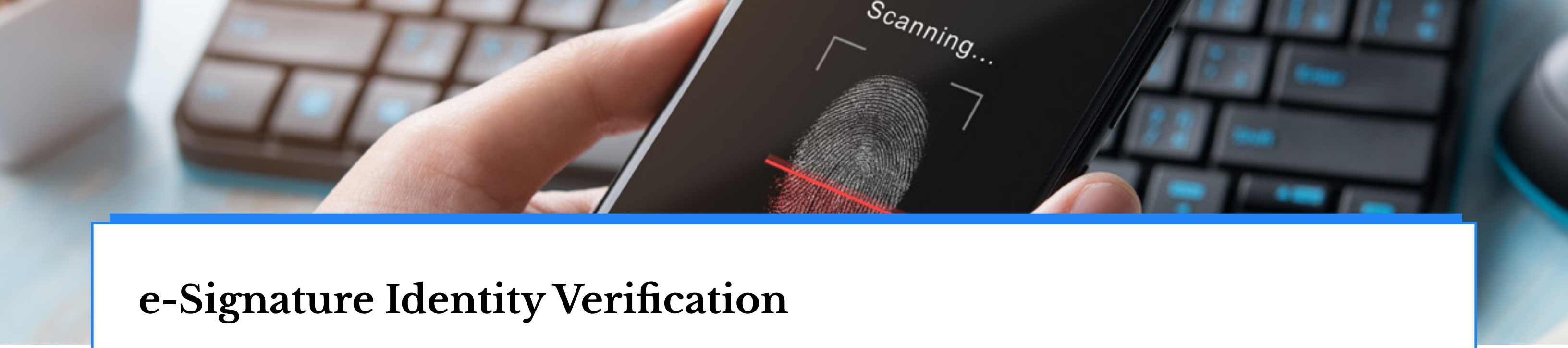
Since a password or PIN is something someone “knows,” there is always a risk of it being forgotten, stolen, or hacked. In order to defend against brute force hacking attempts that seek to guess passwords, cybersecurity experts have advocated the use of increasingly complex passwords. Unfortunately, these passwords are difficult to remember, which leads to people having to write them down or, worse, store them in a computer file that could itself be hacked.

Since biometric data represents something people “are” rather than something they “know,” it is impossible to lose or forget those credentials. They are also much more difficult to steal because they are unique to every individual and cannot be replicated. Utilizing multi-factor biometric authentication, which requires the user to present multiple types of biometric data before their identity can be verified, is also very effective at preventing fraud or unauthorized access. Continuous facial recognition can even authenticate a user on a moment by moment basis to further reduce the risk of fraud and prevent snooping passersby from stealing a glance at sensitive information on the screen. This technology has the potential to revolutionize document security.

> Continuous facial recognition can even **authenticate a user on a moment by moment basis** to further reduce the risk of fraud.

Biometric verification is also quite frictionless compared to traditional authentication systems.

There’s no need for users to keep track of multiple passwords or go through multiple verification steps across different platforms. More importantly, biometric data can be used to create a record that allows organizations to see exactly who accessed sensitive documents or information, which is essential for verifying e-Signatures and authenticating invoices.



e-Signature Identity Verification

With more business being done online, e-Signatures have become increasingly important for keeping deals in motion. However, without proper verification that contracts were sent, received, and signed by the appropriate people, companies could quickly find themselves on the wrong end of legal disputes (as happened in California's precedent-setting Fabian v. Renovate case in 2019). As the suit demonstrated, proving the authenticity of an e-Signature is not always a simple matter, especially when their e-Signature system uses no clear method of authentication to verify who is signing the document.

Biometric e-Signature identity verification technology offers an ideal solution because it can easily demonstrate who actually signed the document and how it was delivered. This is important because if a company cannot actually authenticate the identity of the person signing a contract, it could be exposed to substantial legal action or financial losses. The unique nature of biometric data ensures that the person opening and signing a document is actually who they claim to be.

Fabian v. Renovate

A critical 2019 case relating to e-Signature identity verification, the California Court of Appeals ruled that an electronic signature and corresponding identifying code is insufficient for verifying that a signature is authentic and contractually binding. In order to verify authenticity, additional evidence about the process is required, including:

- Who sent the contract.
- How the contract was delivered.
- Who received the contract.
- How the electronic signature was placed on the contract.
- How the signed contract was returned.
- How the sender's identity was verified as the person who signed the contract.

The Biometric Revolution is Here

Although early uses of biometric technology raised concerns about privacy and whether or not corporations should keep biometric data on file, the security benefits of biometrics have long outweighed the potential downsides. More than 75% of consumers have already used biometric verification in some form, and the majority of smartphones and wearable devices contain the hardware necessary to scan biometric data. Although more than half of mobile users across all age groups have concerns about the way their biometric data is being managed, they are rapidly becoming more comfortable with biometrics and increasingly view it as a “good” technology in the fight against cybercriminals

> **more than 60% of companies are already using biometric authentication** in some capacity while another 24% plan to incorporate it by 2021.

Enterprises were quick to recognize the value of biometrics.

That’s why more than 60% of companies are already using biometric authentication in some capacity while another 24% plan to incorporate it by 2021. With so many employees using their own smartphones in a work capacity, it’s hardly surprising that 46% of workplace biometric use is happening on mobile devices. Since these devices are being used to share sensitive documents over WiFi connections, biometric authentication can be used to ensure that those documents remain secure. With biometric verification in place, access can be restricted to only the document’s intended recipient as their distinctive identity must be authenticated to garner document access.

With consumers becoming more comfortable with the use of biometric authentication, the time is right for organizations to leverage the technology to protect their business from fraud and unauthorized access to sensitive materials. Having top-notch security measures in place can prevent valuable data from being compromised, protecting both revenue and brand reputation in the process. Biometric authentication is a good use case of technology that delivers an unmatched combination of security and convenience when it comes to document security and e-Signature identity verification.

IV. Smart Eye Technology®

At Smart Eye Technology, we've pioneered a new platform that utilizes continuous and multi-factor biometric security to keep private documents secure by blocking screen snooping and prohibiting unauthorized access to shared files. Our revolutionary platform completely eliminates the need for managing easily hacked credentials such as usernames and passwords - and gives users complete control over who can view and access their documents.

In addition to biometric authentication, Smart Eye also provides an enterprise document sharing and access control platform.

Once documents are securely shared, users can change or revoke access as well as decide whether or not the document can be downloaded and shared with others. Real-time notifications create an auditing trail to show when documents are viewed or downloaded. Access credentials can be issued temporarily or even terminated after the fact.

Smart Eye's biometric authentication capabilities bring a new level of security to e-Signatures. Thanks to its unique continuous facial recognition technology, only the intended document signer will be able to open and sign the contract and verify the signer. Signatures are time-stamped and saved along with photo identification to verify the signer's identity.

Protect Your Documents Today

Experience Smart Eye Technology today with a **free two-week trial**.

Available for iOS and Android, the Smart Eye app can be found on the Apple App Store and Google Play. To learn more about how our revolutionary continuous and multi-factor biometric authentication technology can help keep your organization's documents safe and secure, contact our experienced cybersecurity team today.

Download on the App Store

GET IT ON Google Play