Microsys
Smart IT Solutions

(416) 425 0444

HOW SAFE ARE BIOMETRICS?

Analyzing the safety of biometrics.

HACKERS ARE BEATING BIOMETRICS- SHOULD YOU BE WORRIED?

Biometrics is one of the most effective lines of defense you can use against hackers. They are incredibly convenient and allow you to access your devices and bank account with your biometrics. And they appear to be safe too. After all, only you have access to your fingerprint, iris pattern, and facial pattern.

It's clear from top headlines in the news, however, that hackers have caught up with biometric security.

In fact, biometric hacking has become a common way for cybercriminals to access sensitive data. Biometric hacking may allow criminals to bypass conventional security measures such as PIN codes and passwords.

SO HOW DO BIOMETRICS GET BROKEN?

Hackers have several tricks up their sleeves when it comes to compromising biometrics. The most common method is to use a skimmer, a device that can be placed on ATMs and other fingerprint scanner machines. This device logs all information from the finger scanner and then allows hackers to recreate a duplicate fingerprint that can then be used to breach accounts.

Spoofing is yet another strategy that allows hackers to break biometric security. This technique allows hackers to use a fake fingerprint that looks very similar – but not the same - to the real finger pattern to bypass the scanner. This attack is usually done by taking a picture of the victim's finger to make a duplicate of their fingerprint.

Spoofing fingerprints and other biometric information is a relatively straightforward process. One team demonstrated just how easy it was to spoof a fingerprint on a budget of less than $5 using only Photoshop, printer, wood glue, and paper. Fingerprints can also be spoofed as long as the hacker has access to a high-resolution photo and a 3D printer. This usually costs a lot more than $5, but it may be worth the investment if the target is a business owner.

Voices can be spoofed just as easily, thanks to free machine learning models and text-to-speech apps. In fact, voice-deep fakes can be used to convince employees that they are talking to their managers. Remember, "there's more than one way to skin a cat".

THE POWER OF RESIDUAL FINGERPRINTS

This is one trick you probably didn't know was effective: reusing residual fingerprints. Every time you touch a surface, you leave fingerprint impressions behind. And a fingerprint scanner is no different. All a hacker has to do is harvest these prints and use them to break into your devices.

As scary as it sounds, preventing this attack is also relatively easy, albeit rather primitive. All you have to do is wipe down the fingerprint scanner after using it. Make sure to clean all the areas of the scanner that you have touched. This should prevent hackers from stealing your fingerprints and then breaching your accounts.

THE POWER OF RESIDUAL FINGERPRINTS

You should never rely on any standalone tool or technique to protect your IT systems from hackers. The best cyber security suite is a combination of tried and tested methods such as passwords, usernames, OTPs, and fingerprints, among others. The goal is to implement as many additional layers of security as possible to protect your business from hacking.

Here are a few tips you can use to improve your cybersecurity posture.

ROLLOUT AI AND MACHINE LEARNING TOOLS

AI and ML can do what humans cannot: keep up with massive data sets to flag biometrics spoofing attempts. Implementing AI and ML would allow your business to stay one step ahead of cybercriminals. Not only is AI more effective than humans when it comes to flagging biometrics spoofing, but it's also faster.

DON'T USE BIOMETRICS ALONE

As discussed earlier, you should use a combination of verification factors to bolster your security systems. This means creating a zero-trust philosophy when it comes to account management, requiring all users, especially at an administrative level, to provide several verification factors to gain access to their accounts. MFA should be the de facto method of signing in at this point.

AWARENESS CAMPAIGNS

Even the world's best cybersecurity tools are only as good as the humans operating them and phishing scams remain the most effective way of breaching systems. Your best bet is to educate your employees on how to protect their biometric information and not share it with others.

To create a strong cybersecurity awareness culture in your business, you should aim to host a cybersecurity awareness campaign at least once a year. This seminar should provide information over videos, quizzes, surveys, policies, and simulations.

OPT-OUT OF BIOMETRICS (NOT ALWAYS RECOMMENDED)

If you're worried about the security of your biometric data and believe that it may have already been compromised, you can always opt out of it. Consider disabling fingerprint authentication or disabling biometric authentication entirely. This will, of course, vary depending on the device and software.

Most smartphones will let you disable fingerprinting and facial recognition. Social media platforms like Facebook also let you disable biometrics.

KEEP YOUR SOFTWARE UPDATED

The best way to secure your business is to keep your devices updated with the latest software patches. When your device or software vendor notifies you of an available software update, install it without any delays to reduce the opportunity of your device being vulnerable to any security flaws. This is important even if it comes at the risk of lowered productivity for a period of time.

WRAPPING UP

Biometric verification is convenient to use, but like any other cybersecurity measure, it's not 100% secure. Although we have outlined a few vulnerabilities of biometrics, this doesn't mean you should discontinue using them. You should always try to bolster your existing cybersecurity posture by laying them with passwords and multi-factor authentication.

To keep your IT system, devices, accounts, and network safe from hackers, consider hiring managed IT service providers. Our experts at Microsys will provide cyber security services to your business, including round-the-clock monitoring and reporting so you worry about someone breaking into your systems.

Contact Microsys for more information.