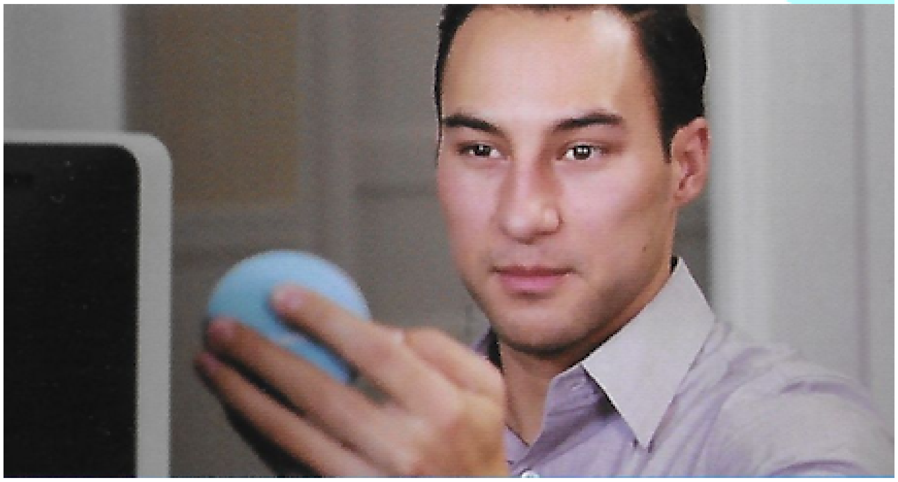
myris™

Worried about Your Computer Accounts' Security?



You can't avoid news stories about computer security breaches. When breaches occur, attackers steal your personally identifying information (PII), such as name, birthdate, and government ID numbers. Criminals use PII to commit identity theft.

Sometimes attackers steal files that contain the accounts and passwords used to access to the website. Passwords are usually encrypted, but once they are downloaded, the criminals apply networks of computers to crack the passwords mathematically. Given enough time and compute power, your password will be revealed.

In this case, the only sure defense is to change your password more frequently than the time it takes the bad guys to crack the password file. But changing passwords frequently means you have to remember lots more passwords. Who needs that?

Do You Get Frustrated with Inconsistent Password Requirements?

In the past, cybersecurity pundits said that you should mix the types of characters in your passwords. Most websites require you to include upper and lower case letters, digits, and punctuation in your password. Every site has different password requirements, mutually incompatible and rather arbitrary.

If you do the math, you will find that longer passwords containing just letters are harder to crack than shorter passwords with mixed character sets. So, cybersecurity experts now say that you should use "pass phrases" – at least 15 letters from a memorable phrase. The problem with this is, how do you remember 100 or 200 "memorable phrases"? Just as importantly, while long passwords are more secure, they're also harder to type.

You can write down all of your pass phrases in a notebook that you keep in your purse or on a few sheets of paper that you keep in your briefcase. That solves the memorization problem, but makes your entire digital life subject to compromise, if you lose your briefcase or your purse is stolen. Longer pass phrases also means more opportunity for typing errors, which means more frustration. Is there an alternative to the password mess?

myris™ is the Solution to Your Password Problems

myris™ looks at the unique characteristics of the iris of each of your eyes and generates an encrypted profile, which it stores on the device To authenticate yourself, myris™ matches that encrypted profile with a scan of your eyes, each time you use it. Once you are authenticated, myris™ submits your encrypted username and password to login to your computer, websites, and password-protected applications. Once you have setup myris™ to work with one of these, you will never have to type another password again.

No two irises are alike – not in twins, not even in the same person. The iris is the colored portion of your eye that surrounds your pupil. It has unique patterns, rifts, furrows, colors, and rings. Your iris remains the same as an adult, so authentication errors are less likely with some other biometric methods.

Cybersecurity experts agree that iris scans are the most accurate biometric identification method available. They are better than fingerprints, palm scans, retina scans, or voice prints. The encrypted profile of your iris is stored in myris™. It is not transmitted over any network, and is not stored in the cloud or on your computer.

myris™

Easy to Install and Use

myris™ is fast and easy to install and to use. To install, first you plug it into a USB port, and then follow the instructions from the setup program supplied with myris™ to generate your profile and ID. Next, you connect to sites and applications, guided by the program. You register usernames and passwords for each one.

To use myris™, you power on your PC, or point your browser to the website URL, or start up the application you want to use. Then, you look into the mirror on the myris™, holding it about a foot from your eyes. The device recognizes you and automatically sends your account and password to the software or website you want to use.

You can carry your myris™ with your laptop or in your briefcase and use it wherever you go. Since the device is so inexpensive, you can even have one for work and one for home.

Case Study #1

I manage a computing lab at a large university. We have many desktop systems sitting on open tables, and anyone can log into them using their university ID. While most tables have two desktop systems, some have only one desktop system, plus one or more specialized devices that are reserved for graduate students in certain departments.

For political and budgetary reasons, we have to keep many systems together in one large room. The high demand for the specialized devices means that we have to keep the lab open almost 24x7. We use the Myris™ system as a cost-effective way to control access to those devices.

Only certain applications can drive the devices. Those applications require passwords, and we use the Myris™ to provide an additional level of security. When a department enrolls a new graduate student, we enroll them with the Myris™ on one of the appropriate desktops. The Myris™ stores the encoded profile of a person's iris scan right on the device

The Myris™ device will store up to five of those profiles. That number of profiles works out just about right for our purposes. The five students negotiate between themselves the schedule of who gets to use the attached devices and when they get to use them.

Case Study #2

I am an IT manager at a medium-sized firm. Our company has a next-generation, flexible office plan. We have private offices, cubicle banks, communal areas, silent rooms, etc. Some of our employees don't have a personal desk. They have a space that they work in for a day, but they might not be in the same space tomorrow.

In a number of situations, we have multiple companies that compete with each other as clients. Given our office architecture, we have to take extra precautions so that one of our employees who works with one company does not inadvertently see, let alone access, the data of one of their competitors. We use several different controls to achieve this. One of them is deploying the Myris™ system.

If a sales or support person is working with one of several competing clients, they are assigned to use certain workstations. They logon to the desktop systems at those workstations using the Myris™ device. The IT department is responsible for assigning employees to workstations so that there is no overlap between our employees who service competing firms.

The Myris™ device is an inexpensive way to physically demonstrate our commitment to the security of our customers' data. We tried other biometric systems, but the iris scan is most accurate. What that means to us is that we don't have to deal with users complaining that they can't login to a system that they have authorization for, and we don't have to worry about unauthorized users seeing data that they shouldn't see.