We know you miss your phone, but will it miss you?

Nomophobia is a distinctly 21st-century phobia, and one that may not be immediately recognizable but the symptoms associated with it will be strangely familiar to millions around the globe. That's because this new phobia refers to the anxiety people experience when being out of contact with their mobile phone.

While this may seem to be a truth self-evident to many, supported by recent studies such as the one conducted by Russell Clayton of the University of Missouri. Clayton's study asked participants to complete word search puzzles in two conditions: In the first condition, they finished the puzzles with their phones on silent in front of them. In the second, they were told the phone was interfering with experiment conditions and were placed across the room. Halfway through, Clayton would ring the participant's phone, allowing it to ring six times before hanging up. The result showed that being unable to answer the phone decreased their cognitive abilities and increased both the participant's blood pressure and heart rate -- key indicators of anxiety.

It's true that the depth of our relationship with our phone varies from person to person, and for many, our phone has become an extension of our brain. We use them to store so much and organize our lives, from grocery lists to memories, and for purchasing widgets to airline tickets. No wonder we're reluctant to part with them. Security companies are taking note and using the fact that we always have our phones on us as an opportunity for secure authentication. It turns out that this can be very effective because each of us interacts with our phones in distinct and unique ways that are naturally resistant to impersonation. This uniqueness can be gathered by various sensors in the device and used to verify identity people in new ways.

Aside from the fingerprint sensor that most people are aware of, smartphones have a plethora of sensors, such as an accelerometer that is used to detect the orientation of the device and phone's movements. Sensors allow manufacturers to build in features such as shaking the phone to changing music. Phones could also include a gyroscope that can be used with the accelerometer to detect rotation of phone, for features like tilting the phone. They also include a digital compass (a magnetometer that detects metals), an ambient light sensor, and a proximity sensor that can detect when the phone is near your head so that it will dim the display. There are also sensors that can detect air pressure and a humidity sensor in some phones, plus a pedometer, heart rate monitor, and even a radiation detector that works via the phone’s camera.

With all the sensory inputs in smartphones today, there is a wealth of data that can be collected and some security companies are targeting these smartphone as a method to collect and analyze physical biometric identifiers. We’re all familiar with fingerprint scans, and perhaps facial recognition. In the future other body areas such as the ear, voice patterns and movements such as walking gait may become common inputs analysed for verification. These methods use the physical biometric to unlock the device and trigger it to send the username and password, or a cryptographic certificate to the authorizing agent for validation of payment or to log in. These approaches require the customer to enroll the biometric and go through a biometric test, placing their finger on the scanner, or taking a selfie, whenever necessary.

Other companies take an ambient, non-intrusive, approach by using passive biometrics and behavioral analysis that reside in the background of the natural interactions the customer is performing across the web visit – whether filling out a form, logging in or performing an action with their browser. These solutions derive their identity intelligence upon what the user does with their device, and how they do it. These systems work by gathering the behavioral information in real-time where it undergoes analysis that uses machine learning to create a profile of the user that is compared to consortium data to determine if the user is behaving like other users in the network provide the authorizing agent an accurate understanding of who is using the phone. The behavioral insights empower the authorizing company the ability to offer great experiences for good users, and instantly intervene anomalous interactions.

Passive biometrics companies such as NuData Security, who pioneered behavioral biometrics, have developed numerous ways to tell whether you are using your device, or whether an unknown party or machine is. By measuring and recording factors such as the angle at which the device is held, the pressure applied to the screen or keys, finger plotting, typing and swiping speed, they build a profile of how and when you interact with your mobile device – without collecting personal information that may compromise your security or privacy. Conversely, by establishing an accurate understanding of your interactions with your device, if behavior emerges that is anomalous and not aligned with your regular activity, behavioral biometrics will uncover it.

This exciting and futuristic new development in the mobile security ecosystem will revolutionize how we interact with brands, enabling them to give trusted users an entirely frictionless experience.

While some people are predicting the end of passwords, the more likely scenario is that passwords will continue to feed useful data into an interdependent, multi-layered and dynamic framework of authentication technologies that combine to form a very accurate assessment of the user behind the device.

While these aspects are of course positives of the industry developments, for the 53% of us who experience anxiety without our phones, the more reliant we are on our phones to provide verification of *who we are*, the greater likelihood of an ever-increasing anxiety associated with our phones should we lose them. Question is, will our phones feel the same way?

____

About the author:
Robert Capps is the vice president of Business Development for NuData Security. He is a recognized technologist, thought leader and advisor with more than 20 years of experience in the design, management, and protection of complex information systems – leveraging people, process, and technology to counter cyber risks.