For secure access, PASSWORDS ALONE DO NOT WORK.

How multifactor authentication can provide a higher level of security.

BACKGROUND

The *2013 Data Breach Investigations Report* assembled by the Verizon RISK team in conjunction with 19 global partners analyzes 621 data breaches, 47,000+ reported security incidents, and at least 44 million compromised records in 2012. Verizon has been researching and analyzing data for more than nine years.[1] The pace of security breaches has not decreased despite advances in security measures and intrusion prevention technologies. Quarter-by-quarter, hacking attempts are increasing exponentially. According to a report compiled by the Internet Crime Complaint Center (IC3), (a joint venture between the FBI and the National White Collar Crime Center), the following statistics indicate the number of complaints reported to the center and the financial scope of the problem:

- Total complaints received: 289,874
- Complaints reporting loss: 114,908
- Total Loss: $525,441,110
- Median loss for those reporting a loss: $600
- Average loss overall: $1,813
- Average loss for those reporting loss: $4,573

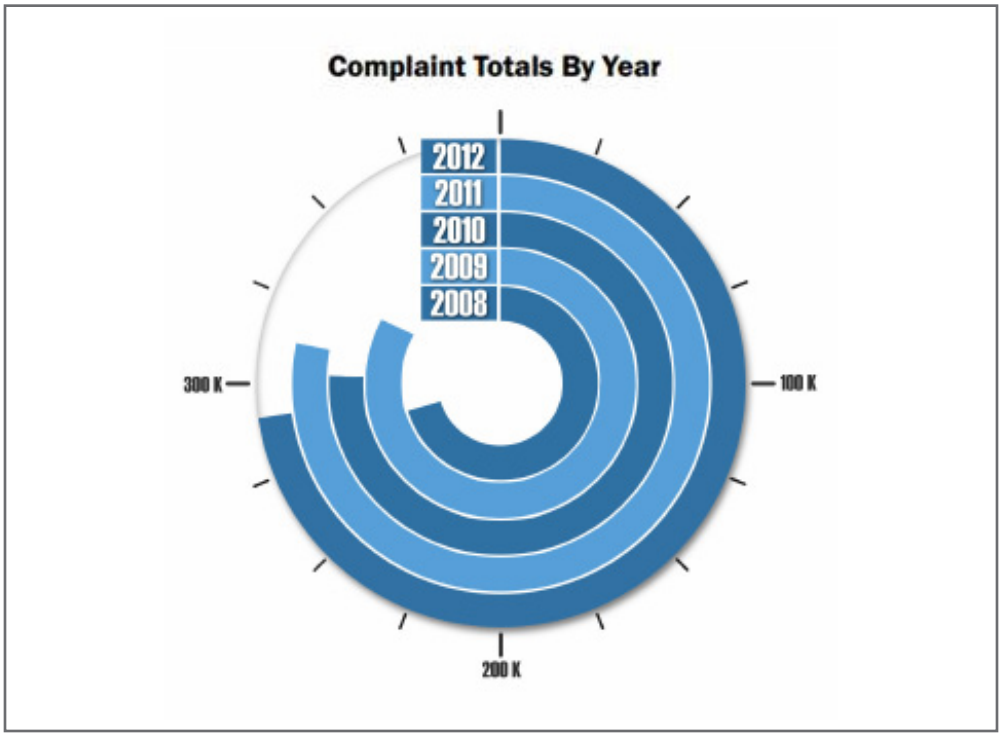

Figure 1. Complaint totals per year reported to IC3. Source IC3 Report. Used with permission.

1 Verizon, *2013 Data Breach Investigations Report*, page 4

How are they breaking in? According to the 2013 Data Breach Investigations Report, more than 75 percent of breaches come from compromised credentials.

Keep in mind—these are numbers of reported successful breaches to the IC3.[2] The numbers of incidents may be much higher, as companies are reluctant to report attacks that they warded off or partially successful breaches in their security systems. In addition, not all countries report incidents, and reporting is entirely voluntary. Many private businesses may not disclose to the public any breach they encounter at all. Nonetheless, the key take-away from the IC3 report is that nearly half of all incidents result in financial losses. The Data Breach Investigations Report (DBIR), as comprehensive as it is, confirms recorded data disclosures from only 27 countries.[3] That means there are far more breaches worldwide than either the DBIR or IC3 combined have documented. The vast majority of breaches come from outsiders: 98 percent in 2011 and 92 percent in 2012 according to the DBIR.[4] More than 75 percent of these breaches come from compromised credentials (user ID and password). The reason is scale. More and more hackers and better password and credential hacking tools are available now. The undeniable trend is toward orchestrated and coordinated attacks coming from increasingly sophisticated and highly organized criminal and state-sponsored sources rather than individual hackers.

NEW VULNERABILITIES

If hacking into corporate sites over the Internet were not enough, the widespread adoption of smart phones, tablets, and laptops to access company data has introduced a whole new world of vulnerability challenges for IT security professionals. Again, the frontline defense has been to make sure passwords and credentials are not compromised while using these devices. Many organizations are just now implementing corporate security policies for BYOD. Unfortunately, many still have no formal policies, procedures, or safeguards in place.

Cloud-based applications and services, whether private and housed internally, or hybrid cloud services based on secured, outsourced provider platforms, also represent a significant enterprise concern. In fact, a 2013 study conducted by *CIO Magazine* concluded that although 82 percent of respondents would host at least some of their corporate data on an outsourced cloud service, 54 percent cite security as a high priority, particularly perimeter security.[5] Again, password and credential compromises are the easiest, low-hanging fruit for hackers to gain entry to corporate clouds.

35,000%

THE AMOUNT ANDROID MALWARE GREW BETWEEN 2011 AND 2012.

Lastly, organized and well-funded criminal and state-sponsored hackers have better tools and methods available to them to overcome most password and credential safeguards. For example, according to news reports from the Middle East and Europe, highly organized and well-funded Russian hackers have recently started an underground economy of providing "malware-as-a-service," including affiliate links, "customer" (i.e., freelance hacker) support, and a continual stream of new malware code for racking up millions of dollars in fraudulent SMS charges. Using off-the-shelf graphics processors (GPUs), a researcher in Oslo, Norway recently demonstrated a system that could produce over 348 million password hacks (or hashes) per second—this takes brute force hacking to a whole new level.[6]

THE PROBLEMS WITH PASSWORDS

The biggest problem with computer passwords is that we inherited them from legacy computing systems. Password logins began in the early days of mainframe computing; users would login to their terminals with their IDs and provided passwords to access data. From there, the "technology" of passwords migrated to LANs. In both cases, the security is localized—someone would need to be onsite, have proper clearances and proper credentials to enter the system. We no longer live in that world. Everything is now connected, virtualized, and globally available.

The most "deadly" and costly password hacks are wholesale thefts of a company's entire database of customer and/or employee user IDs and passwords. Armed with potentially hundreds of thousands of stolen passwords, criminals can then quickly reap cash or data. Whether the motivation is financial or espionage, the results can be devastating. But it gets worse.

2 IC3, *2012 Internet Crime Center Report*, May 2013
3 Verizon, *2013 Data Breach Investigations Report*, page 14
4 Verizon, *2013 Data Breach Investigations Report*, page 15
5 Olavsrud, *How Secure is the Cloud?*, March 2012, CIO www.cio.com/article/703064/How_Secure_Is_the_Cloud_IT_Pros_Speak_Up
www.cnmeonline.com/news/malware-as-a-service-blossoms-in-russia-vendor-research-finds/
6 The Security Ledger, *New GPU Monster Devours Passwords in Seconds*, December 2012, https://securityledger.com/?s=GPU+monster

The following are a few of the most common flaws in password use by individuals and companies alike:

One password for multiple sites. Most people are not inherently lazy when it comes to creating and using passwords, they are inherently busy and forgetful. Because of this, they tend to use the same passwords across many sites for the sake of convenience. It saves them time and clicks. Once their password is compromised at one site, however, it is easy for hackers to try victim's IDs and passwords on multiple sites, gaining deeper and even more damaging access to personal and corporate data.

Easy passwords. Most people pick passwords that are easy for them to remember. Given that the number of passwords users must commit to memory these days, this is no surprise. This also makes them easy to hack. In fact, according to Mark Burnett, author of *Perfect Passwords*, 91 percent of all people use a variation of the top 10,000 most commonly used passwords. An unbelievable number of people simply use "password" or "password123," for example. If required to use special characters, few people use symbols that are easily confused, such as commas, periods, or semicolons. Therefore, the most commonly used symbols are: !@#%?.[7] These commonalities make password hacking even more easy to accomplish.

The written word. Enter just about any corporate cubicle and you'll no doubt find written passwords in the occupant's top desk drawer, or amazingly, even pinned to a cubicle wall. Some people carry them on slips of paper in their wallets or purses—far safer, but still easy to read and copy down if the person leaves them unattended for a time. Those slips of paper can easily get lost too.

Infrequent password changes. Many companies wisely require mandatory password changes at set time frames—usually three to four months. The problem, again, is that people choose simple passwords, easy to remember, and easy to change. So "password123" becomes "password456" and so on. Even worse, many companies have no mandatory password change policies at all.

Phishing for credentials. Many individuals fall prey to phishing attacks. They may receive an email, supposedly from their bank, a popular online shopping destination, or a social web site asking that they login using a link in the email to check their account or reset their password. These emails have become increasingly sophisticated, using official company logos, and professional-looking forms and privacy statements. Many people fall prey to these attacks, and hackers can send out hundreds of thousands per day.

Key-loggers and malware. If you open an email attachment you can instantly introduce malware (stealth software) onto your machine. This malware may not be immediately noticeable; in fact hackers motivated by financial or data theft count on the malware's undetectable nature. In password hacking situations, the malware logs all keystrokes entered by the user on the infected machine and forwards the captured keystrokes to the hacker's site where they are inspected for IDs, passwords, or even worse, sensitive data itself.

Brute force for complex passwords. Even if users follow all the best practices for password creation, change, and do not open attachments or fall for phishing schemes, hackers have the resources and computing power to attack systems with brute force—on the order of millions of hashes per second. These attacks are usually carried out at the system level to gain administrator privileges. Even the most complex and strong password strings are susceptible to brute strength or "crowd hacking" approaches.

THE BOTTOM LINE: PASSWORDS ALONE FAIL, AND RECENT EVENTS PROVE THIS

The bottom line is that the hackers—by brute force, their sheer numbers, and increased technological expertise—can compromise a vast majority of user IDs and password combinations. Even the most sophisticated online companies have fallen prey. In just the last year we've seen reports in the press of major online companies and brands experiencing data breaches and password compromises. In some cases literally millions of user IDs and passwords were compromised.

The cost to companies that experience wholesale theft of credentials to hackers is enormous as they scramble to re-instate new passwords, IDs, and add better security measures. Even minor breaches or "password forgetfulness" ties up corporate IT helpdesks—time better spent improving systems. If even one system administrator ID and password is compromised, an enterprise can suffer a devastating loss of intellectual property.

The widespread adoption of smart phones, tablets, and laptops to access company data has introduced a whole new world of vulnerability challenges for IT security professionals.

USE A VARIATION OF THE TOP 10,000 MOST COMMONLY USED PASSWORDS.

7 Burnett, *10,000 Top Passwords*, http://xato.net/passwords/more-top-worst-passwords/

The most "deadly" and costly password hacks are wholesale thefts of a company's entire database of customer and/or employee user IDs and passwords. Armed with potentially hundreds of thousands of stolen passwords, criminals can then quickly reap cash or data.

For these reasons, many industry analysts, security experts, and many other leaders in the technology sector, recommend a wholesale conversion to a technology that can withstand the online onslaught of password hacking: Multifactor Authentication.

WHAT'S NEEDED: MULTIFACTOR AUTHENTICATION

Multifactor authentication requires a combination of at least two of three factors to provide a higher level of security than legacy-based user ID and password systems. The factors are:

- A knowledge factor (Something the user knows)
- A possession factor (Something the user has)
- An inherence or physical identity factor (Something the user is)

Something the user knows can be a PIN, a pattern, and yes, even a password. Something the user has can be a smartcard, a hardware device, or a cell phone. Something the user is usually refers to a biometric, such as a fingerprint or retinal scan.

Of all three authentication factors, biometric scanning is of course the most expensive and difficult to implement on a wide scale. For this reason, most multifactor authentication systems rely on knowledge and possession factors.

HARDWARE MULTIFACTOR AUTHENTICATION

Multifactor authentication has been around a long time, and most rely on hardware tokens to fulfill the possession factor of the system. Usually in the form of a USB or a key fob device, these hardware devices use one-time passcode generation. Any of these hardware devices display a time-synchronized code that the end user types into his or her device (laptop, smart phone, or tablet). This code is transmitted to the enterprise for comparison with a code calculated in the enterprise's One-Time Passcode (OTP) server. If the code entered by the end user matches the server-generated code, the end user has successfully authenticated. The server uses sophisticated algorithms to generate this one-time passcode, usually a string of numbers, which the user must then enter during that login. When this is combined with the user's PIN (something the user knows), multifactor authentication is complete. The OTP itself is not used again—there is nothing to steal or hack.

In its *Bringing Multi-factor Authentication to the Masses*,[8] the Frost & Sullivan analyst research report points out that hardware OTP is widely accepted, field tested over many years, and has an extremely low likelihood of compromise, as the login is dependent on a one-time, disposal passcode sent to the OTP device. The devices themselves are encoded and tamper proof as well. Nothing is stored on the server or end-user device, and the PIN is in the user's head. In fact, ATM access is nearly identical in its implementation, and is used securely millions of times a day throughout the world.

Hardware OTP tokens add a burden, however. It is another device the user must carry; it may get lost; and, in extreme circumstances, it could break. Replacement takes time. This reduces productivity, increases costs, and frustrates users and system administrators.[9] Other cost factors, according to Frost & Sullivan, include the following:

- **Active and time-sensitive participation.** Attention is required by the end user to enter the OTP correctly and within a time window that is synchronized with the code generated by the enterprise OTP server. For on-the-move individuals, this juggling effort presents obvious challenges.
- **Cost.** Multiple costs are present with hardware OTP tokens: the hardware device, the enterprise OTP server, and management time in provisioning and de-provisioning hardware devices, end-user account management, and server oversight.[10]

SOFTWARE MULTIFACTOR AUTHENTICATION

Software multifactor authentication is identical to special-purpose OTP hardware devices except that the key generation and one-time passcode display is secured on the user's device—whether it's a laptop, smart phone, tablet, or even a PC. This serves as the "something the user has" criteria. It has the advantage over hardware tokens because it costs less, is universally available, and could be used with a simple 4-digit, easy-to-remember PIN, just like consumer ATM cards.

8 Suby, *Bringing Multi-Factor Authentication to the Masses*, May 17, 2013, page 4
9 Ibid
10 Suby, *Bringing Multi-Factor Authentication to the Masses*, May 17, 2013, page 5

The downside is loss or theft of the user's device, yet still, the thief would need to know the user's PIN—or spend a tremendous amount of computer time cracking the software-based authentication system. Unless the PC or phone is a high-value target, most hackers would not waste the energy; in the meantime, the loss or theft would no doubt be reported by the user quickly. Some vendors are already shipping devices with hardware-embedded chips on smart phones and laptops, making any hacking difficult.

Online vendors such as Amazon, Best Buy, and others have calculated that adding clicks and complexity to the online buying process results in lost revenue in the form of abandoned online shopping carts. The idea of correctly entering an OTP in the time period allotted complicates even the use of software-based multifactor authentication. Therefore, multifactor software solutions need to be as frictionless as possible, in fact, almost invisible to the end user.

IS MULTIFACTOR AUTHENTICATION VULNERABLE?

Yes, even multifactor authentication is vulnerable, but far less so than our current legacy ID/password systems. In the Data Breach Investigations Report, of the thousands of attacks studied, less than one percent involved compromised multifactor identification. "In underground communities we're seeing a lot of chatter focusing around mobile, specifically with phones," Daniel Cohen, Head of Online Threats Managed Services at RSA told *BuzzFeed* in a recent interview. Cohen notes a 35,000% percent growth in Android malware between 2011 and 2012, from 1000 samples to 350,000. "We're seeing apps that will steal your contacts off your phonebook as well as applications that are programmed to steal SMS messages. These programs hide the messages from the users, so you'll never even know you received the SMS," Cohen said.[11]

Multifactor authentication requires a combination of at least two of three factors to provide a higher level of security than legacy-based user ID and password systems.

At this time, virtually all mobile threats to multifactor authentication have come from 1) malware that a user has downloaded, or 2) visiting a corrupt web site that injects malware. Devices with good malware scanning software and steering clear of unfamiliar web destinations are a way to avoid these threats. In addition, many browsers are now "malware-aware."

No security measure is ever 100 percent effective. Businesses, consumers, and software developers must constantly balance cost-versus-risk-versus-convenience when protecting themselves and their systems. Seat belts are a perfect analogy. The least costly "seat belt" would be a simple rope or string tied across your lap. Easy to do, so it fits the convenience category. It certainly is cost-effective, but it definitely gives you very little protection. (Did you tie that knot tight enough?) A nylon lap belt—the first to be used in automobiles—proved to be cost-effective, but didn't prevent head and neck injuries. The shoulder-lap belt combination we commonly use now does a good job at reducing head and neck injuries, is still very convenient to use, and is not very costly. Moving up the scale of seatbelts for even greater protection quickly escalates cost and introduces inconvenience—such as the metal threaded, tri-buckle harnesses used in race cars. These provide the best protection, but at far too much cost and certainly far less convenience for drivers and passengers. At that point we've crossed the threshold of acceptable cost and inconvenience.

NO SECURITY MEASURE IS EVER **100% EFFECTIVE.**

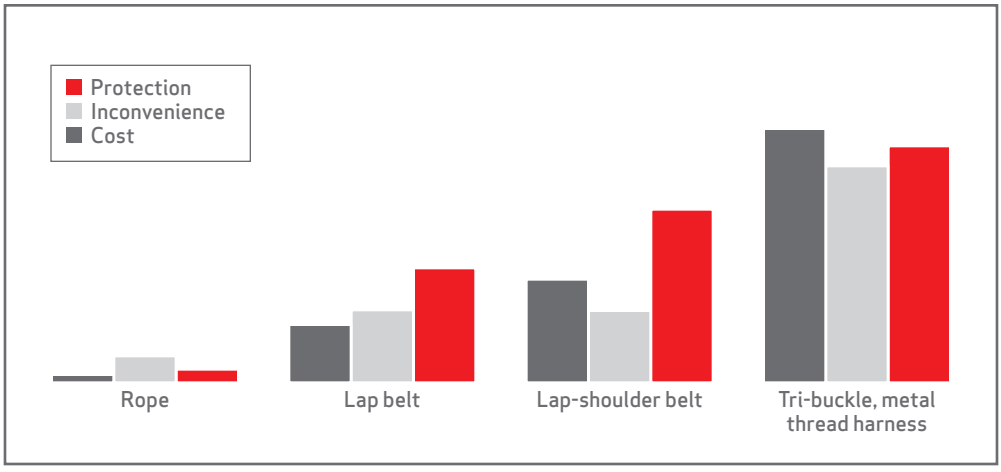

Figure 2. Cost-convenience-safety trade-off factors

11 BuzzFeed, www.buzzfeed.com/charliewarzel/why-two-factor-authentication-wont-stop-our-security-nightma

Universal Identity Services, delivered via the cloud, provides multifactor authentication that allows people to quickly and easily pair something they know (a password or unique code) with something they have (a device) for secure, high-assurance access to systems, applications, and sensitive information.

To augment safety even further, therefore, the car industry adopted air bags instead. Software-based multifactor authentication, augmented with strong perimeter protection, good malware detection and blocking tools, is the same type of dual-technology in action. Cost, convenience, and security come together for a far more robust system than user IDs and passwords ever can.

THE VERIZON SOLUTION: UNIVERSAL IDENTITY SERVICES

With millions of customers, Verizon has considerable experience and depth with identity validation and data security. Universal Identity Services provide multifactor authentication that allows people to quickly and easily pair something they know (a password or unique code) with something they have (a device) for secure, high-assurance login. Delivered via the cloud, it helps organizations reduce risk by providing the right people with access to systems, applications, and sensitive information. It not only helps organizations protect their brands and assets, but it also makes it easy for people to protect their identities with strong authentication. With Universal Identity Services, businesses can collaborate with confidence and deliver web services quickly and securely.

Verizon's Universal Identity Services customers benefit from the following:

- Overcome the business and technical barriers of adopting multifactor authentication
- Deploy authentication systems that fit each business quickly and efficiently
- Control infrastructure and management costs

Since Verizon's Universal Identity Services are vendor-agnostic, multifactor authentication methods can be easily deployed on the following devices:

- Smart phones
- Tablets
- Laptops
- Desktops
- Land lines

Figure 3. Verizon mobile phone-based OTP

Because Verizon's suite of services is cloud-based, its solution is cost efficient and easy to implement when compared to hardware-only or standalone authentication services companies must deploy and maintain on their own. Similarly, the management of the entire multifactor authentication service is left to Verizon's experienced staff and technicians, relieving organizations of many of the complexities and time-consuming management of user authentication systems. As improvements in functionality, features, and particularly security are developed and deployed, customers do not bear the burden of additional equipment costs.

FRICTIONLESS CUSTOMER EXPERIENCE AND RELIABILITY

Verizon offers organizations and their users a simple, flexible solution for reaping the benefits of cloud-based multi-factor authentication. Universal Identity Services reduces the friction of secure login, and the complexity of data access at all levels. By providing alternative methods of identity verification and second-factor login, high assurance authentication becomes more convenient for users and gives organizations a powerful layer of security control.

In addition to security and reliability, Verizon maintains a high availability multifactor authentication platform. Universal Identity Services helps customers address security compliance requirements such as the Federal Information Security Management Act (FISMA), the PCI Data Security Standard and the DEA Rule for Electronic Prescriptions for Controlled Substances (EPCS). In addition, Verizon was named Gartner's Magic Quadrant Leader for the following:

- Leading Managed Security Service Providers, 2011 and 2012
- Leading Cloud Infrastructure Leader, 2011 and 2012
- Leading Managed Hosting Provider, 2012 and 2013

VERIZON UNIVERSAL IDENTITY SERVICES BENEFITS

Helps Improves Security. According to the 2013 Verizon Data Breach Investigation Report[12], four out of five of attacks would be thwarted using multifactor authentication. Verizon was the first Identity provider to earn Level 3 Identity Credential and Access Management (ICAM) certification. This means Verizon can address the risk management needs of even the most demanding businesses and government agencies. Not all applications are created equal nor require the same level of

12 Verizon, *2013 Data Breach Investigations Report*

security. Therefore, Verizon offers choice: customers can choose from three different levels of identity strength to accommodate secure login requirements for various applications, data access, and web-based services.

Provides a Convenient and Flexible User Experience. Verizon has significantly reduced the complexity associated with traditional second-factor authentication solutions. People can get a Universal ID using a simple, online self-enrollment process or using their social media identities. Unlike most two-factor solutions, Verizon allows users to choose from a variety of devices they already own for second-factor, such as a smart phone, tablets, computers, or even landlines. The Verizon mobile application makes it extremely convenient for users to login with merely one touch, eliminating the need to type digits to submit a one-time passcode. Users can also scan a QR code for second-factor authentication. Best of all, once a user has a Universal ID they can use it across multiple participating applications and web services, eliminating the need to re-enroll or create even more usernames and passwords.

Simplifies Identity Management. For organizations, Verizon's Universal identity Services reduces the complexities of securing and managing digital identities across the enterprise—from verifying, creating, and managing IDs through to de-commissioning identities. This controls IT management costs and reduces complexities. In addition, Universal Identity Services enables fast, easy, and secure sharing of data among business partners and other trusted identities. For example, healthcare providers can use their Universal ID's to access multiple sites, applications and e-Health records. Partners and customers alike can save time, manage costs, and gain strong authentication.

Accelerates Time-to-Deployment. Universal Identity Services provides repeatable, on-demand enrollment and authentication processes, and secure login capabilities that can be quickly and easily rolled out to millions of users, business partners, vendors, and government agencies. Deployment and management of users and systems is greatly simplified.

Controls Costs. Because Universal Identity Service is delivered in the cloud, Verizon eliminates the need for specialized hardware or software IT expertise. Competitively priced, it also helps to control operating costs associated with managing digital identities, audit preparation, on-boarding new customers, and helpdesk queries.

Provides High Availability, Scalability and Security. Universal Identity Services are housed at geographically dispersed and physically hardened Verizon data centers and are designed to accommodate hundreds of millions of users. Verizon built its system from the ground up to address strict security standards, including U.S. Federal agency guidelines, requirements, and mandates.

The cost to companies that experience wholesale theft of credentials to hackers is enormous as they scramble to re-instate new passwords, IDs, and add better security measures.

SUMMARY

We no longer live in a word of computer terminals and isolated LANs. With our highly connected, global communications systems, we have seen a tremendous boost in productivity, commerce, and continual innovation, worldwide. That interconnectivity, when using user IDs and passwords for access, has introduced a multitude of risks and will remain vulnerable if we do not upgrade our security systems to match our current technology. Passwords alone are not the answer: they are the problem.

Multifactor authentication in any of its forms is a giant step in the right direction. The challenge is to make systems more secure yet not add burdensome costs and inconvenience. Any adoption of multifactor authentication should be universally adaptable across a multitude of current and new devices while maintaining a high level of security and reliability. Cloud-based authentication services can provide that type of security and adaptability. Because customers do not need to maintain an on-site authentication system or invest in a multifactor authentication hardware and software infrastructure, they not only have choice in the type of authentication service they use, but also can effortlessly make changes or upgrade when needed. Cloud-based authentication service, such as Verizon's Universal Identity Services, keeps costs low through a shared yet secure environment, and customers automatically reap the benefits of any Verizon infrastructure improvements with no added CAPEX.

Finally, just as customers choose the "easiest" passwords to remember for convenience sake, multifactor authentication should introduce better protection with even less difficulty than remembering and changing passwords. Customers can then conduct online activities and business without remembering anything more than a 4-digit PIN, and in the process, toss out those scraps of paper with scribbled and easy-to-hack passwords.

verizonenterprise.com