Authentication for the Next Generation

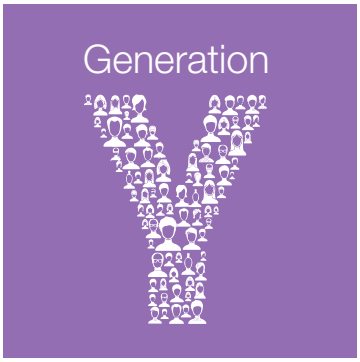
How Gen Y is changing the way we protect our digital lives

By David Strom

VASCO®
THE AUTHENTICATION COMPANY

Table of Contents

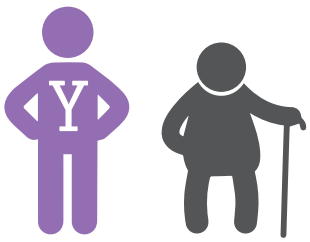
Foreword



The new “my way” work style and the demand for on-the-go access to any service from any device and virtually any location requires that you bring your best encryption game with you when you’re on the move. While you can be somewhat blasé about a corporate or home network that is under your control, when you leave home, you need to bring two things – your device of choice, and your encryption gear.

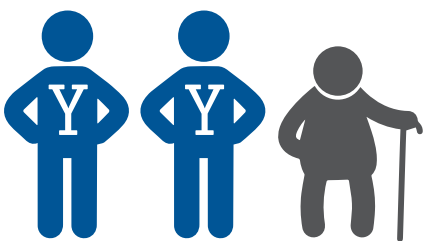
This is especially true for the group of people often labeled Gen Y, or 20-somethings. Why? Because they are so digitally native and so used living their lives with instant access to their money, their friends, really anything that they do. As they are so steeped in technology, they tend to forget that there are lots of folks online who want to steal their identities, empty their bank accounts, and cause other havoc with their digital lives.

In fact, some call Gen Y the new threat vector. But while Gen Y certainly is a great target of opportunity for digital thieves, just because they are so connected, they are also great targets of opportunity in the other direction too: They are more willing to adopt, embrace and promote the use of powerful new technologies, and demonstrate how they’re using new innovations to protect themselves in an online world.



59 %
OF MOBILE BANKERS
ARE 18-34

MEMBERS OF GEN Y ARE
TWICE AS LIKELY
TO BE A MOBILE BANKER



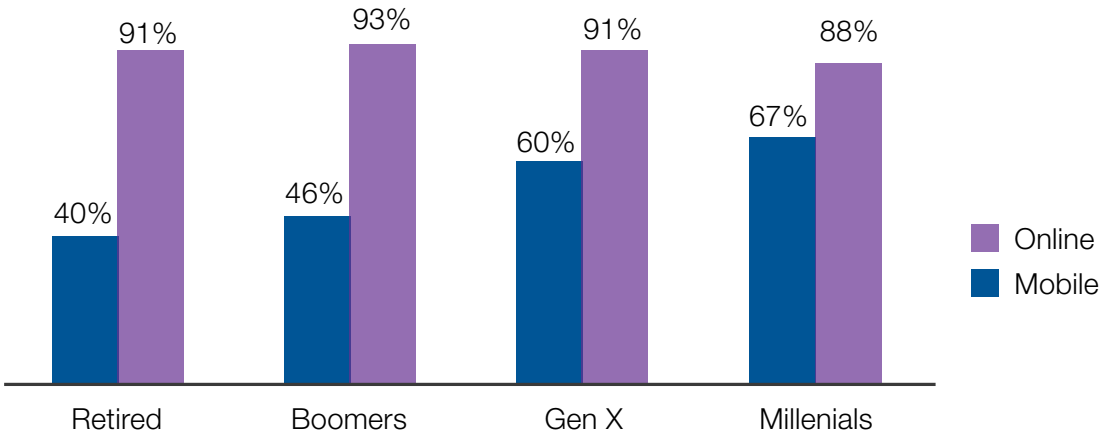
Gen Y’ers are twice as likely to use mobile banking apps, and nearly 60% of the users of mobile banking apps are between 18 and 34 years old.
(Source: Mountain America Credit Union)

Generation Y taking over

And as each new generation become more technologically advanced, banks and other service providers must recognize the importance of rapid development and deployment cycles for mobile offerings in response to these new expectations.

Part of the challenge is that Gen Y has raised the bar on these requirements. They are much more likely to use mobile banking than their elders, and more likely to go elsewhere if banks do not offer the mobile services they desire.

Mobile Banking is the Future



Consumers who are “currently using” or “considering using” online or mobile banking services

When it comes to protecting themselves and their sensitive data, Gen Y is expecting a lot: Security solutions must be easy to use, integrated into devices that they already carry (think smartphones and smart watches) or built into their apps, and even more secure. And one of the biggest ways that Gen Y are staying secure in their digital lives is through the use of innovative authentication technologies.

To understand how new technologies are addressing the needs of Gen Y, we first need to explore the evolution of authentication. How has authentication changed to meet the needs of users? What are the risks involved when we travel and stay online? What solutions are currently available? How can we use them to strengthen our authentication?

Source: PwC, UK

Evolution of the Token

We certainly have come far with authentication devices in the past 25 years. Back in those days of yore we had these little hardware tokens that could fit on our keychains and had small LCD screens. When you pressed a button on the token, you would get a one-time password (OTP) that would be used to encrypt various connections, such as authenticating to your corporate network or your bank or other Internet conversations. They were a clever approach at the time.

Since those days there have been a number of innovations with authentication, and it has evolved into a variety of new and exciting form factors. Some authenticators now come with a small numeric keypad that ask you to type in a PIN code. Others have USB connections so you can directly connect them to your PC. Some offer QR codes that generate unique cryptogram images instead of OTPs.

And the hardware itself has evolved into various software versions that accomplish the same thing. There are “soft tokens” that run on your smart phone and generate OTPs that mimic the traditional key fob tokens. And a number of security vendors and online applications make use of other factors, such as sending your phone a text message with the passcode or using various biometric methods such as voiceprint ID or using the built-in fingerprint sensors that now come on many of the more modern phones.

How Vulnerable are You? Very.

Because static user names and passwords are so vulnerable, especially outside a corporate network, authentication tokens were an important innovation. This is because people are far too trusting, and do silly things besides. And today, because many of us – including Gen Y – are so used to running our digital lives whenever and wherever we are, we tend to forget that we can be exposed under certain circumstances. Here are just a few scenarios that should scare you:

The Post-it scenario

Many of us have too many passwords to remember, and write them down on a sticky note that is then attached to the top of our monitors. It is almost too comical, and indeed a recent documentary on the British Railways featured a hapless worker with a prominently displayed username and password that had lots of airtime on the BBC. And to make matters worse, the password was 'password3.'

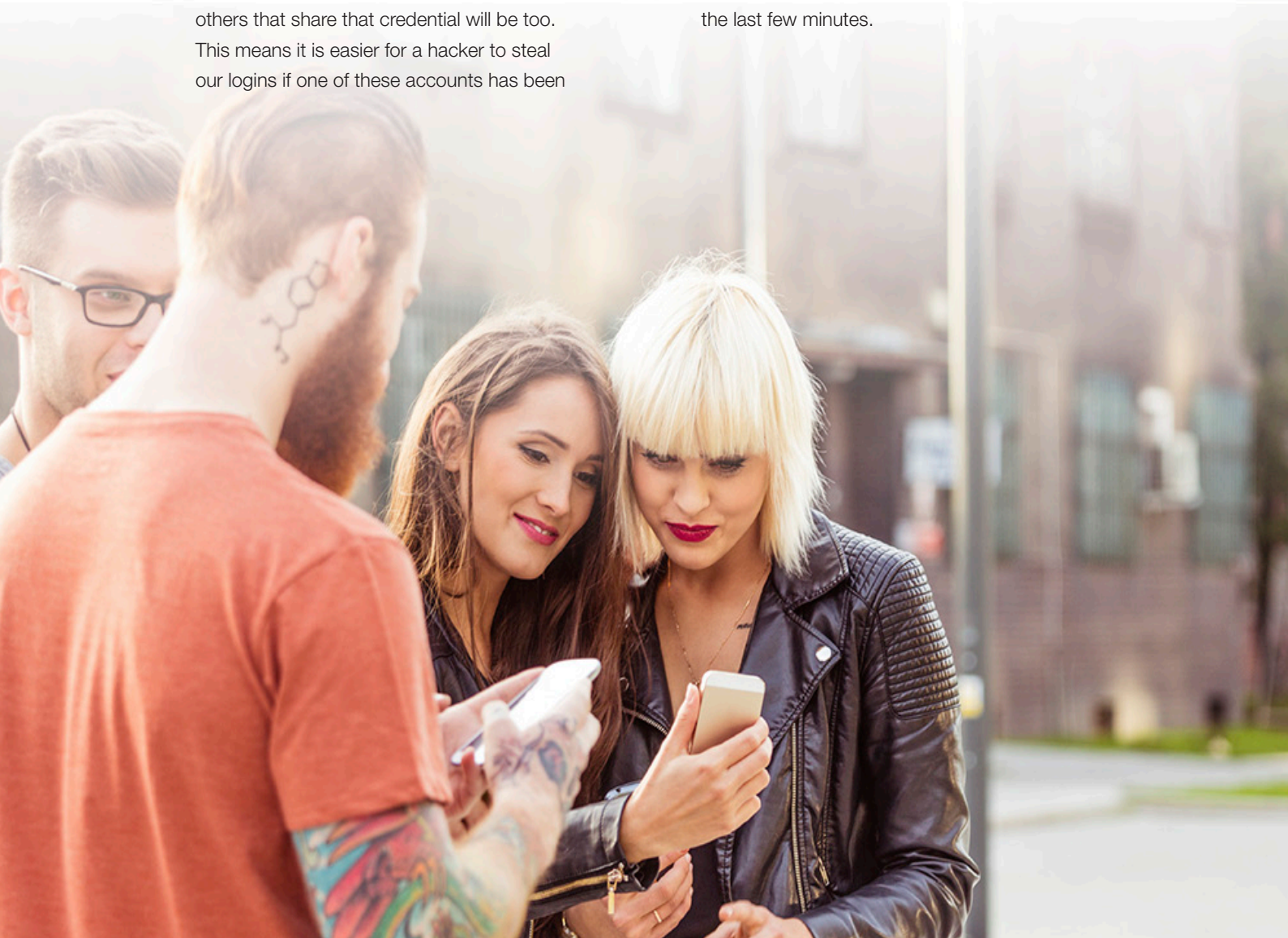
Open file shares

To make our computing lives easier, many people share files from their laptop across their home or work networks. Nothing wrong with that, until they forget that their file sharing is still on when they travel. This means that anyone on the same network in their hotel or coffee shop can view all of their files. Many hotels don't properly secure their networks, and so when you sign in there everyone connected is now seeing your file shares. Go to any center city convention hotel today and within a few minutes you can collect PowerPoints, secret documents, and business plans on just about any industrial topic. And you don't need any skill, other than showing up at the right time and place.

Insecure logins
Many people don't realize that their online/ mobile traffic can be easily intercepted, especially traffic that doesn't use Secure Sockets encryption. This means that they sign into their corporate network remotely and someone can steal their login credentials if they are listening or capturing the traffic.

Shared passwords across various Web and Mobile Services
This is a common situation: we all have too many passwords and most of us do the absolute wrong thing by reusing one "standard" password to gain access to many different accounts. If one account is compromised, all others that share that credential will be too. This means it is easier for a hacker to steal our logins if one of these accounts has been breached. On top of this, passwords are poorly chosen and can be easily guessed either with some knowledge of the individual (a pet's name or a favorite sports team) or through specialized cracking programs that can compare passwords with dictionaries.

VPN issues
A Virtual Private Network is a good way to protect your traffic, since it encrypts everything that comes out of your computer across the Internet. Yet many of us don't both with a VPN because it takes time to setup, or it can add latency to our connections, or it is just too much trouble if we want to just quickly check and see if we got a particular email message in the last few minutes.



Authentication Today

When it comes to authentication of their online lives, Gen Y wants the same kind of effortless and built-in functionality that they get when they check their texts on their connected watch. Look at what has happened to the ATM. Back in the day, they were considered a big innovation and saved a lot of time that would have otherwise been spent waiting inside the bank for a teller to dispense your cash. But now even ATMs themselves are dated, giving way to touchless payments and mobile apps that not only can tell the barista what our favorite coffee drink is, but will instantly deduct payment from our account, with a single swipe of a mobile phone.

The evolution from ATM to cardless payments is typical of how Gen Y is maximizing their technologies. That is why when it comes to authentication, they are attracted to newer options that are more secure, less disruptive and even easier to use. VASCO Data Security, a global leader in authentication, has developed some advanced authentication solutions that meet the demanding requirements of tech-savvy Gen Y. VASCO solutions make data more difficult to steal, while at the same time making online and mobile services even more convenient to use.

CrontoSign Visual Transaction Signing

A series of scanning-based algorithms is a new twist on the old QR codes. VASCO's patented CrontoSign is available in both hardware and software form factor. Hardware devices contain a camera, which automatically scans and decodes an encrypted image containing transaction data, and then presents the data visually to the user for verification.

In addition to offering one of the most user-friendly experiences in transaction protection, VASCO CrontoSign increases security by providing "sign what you see" capabilities to the user, while creating mutual authentication between the user and the service provider for the strongest protection against targeted Trojan attacks, including Man in the Middle (MitM) or Man in the Browser (MitB).

DIGIPASS 760 CrontoSign scanner

Bluetooth-Enabled OTP

Bluetooth-enabled devices (or software tools) can generate the OTP but can transmit the password via a Bluetooth connection as an example. This way an OTP fob, such as the VASCO GO 215 can send the OTP directly to the app, so the user doesn't have to type in the password. This is just one way that a Bluetooth device can secure a transaction and transmit the information to a more hardened environment for subsequent validation.

DIGIPASS GO 215 Bluetooth

Authentication without actual user-initiated authentication

The idea here is to build in authentication as part of the web or mobile application itself, to secure the integrity of the application, and protect the entire transaction from any exploit. For example, VASCO DIGIPASS for Apps is an SDK that turns any app developer into a security expert, enabling them to protect the entire mobile app ecosystem (application, device, platform and user) with a single integration.

DIGIPASS
for APPS

Risk-based methods

With risk-based authentication, access and transaction decisions are based on a dynamic series of circumstances. These count as the additional authentication factor, rather than rely on a particular set of tokens or pieces of smartphone software. Access to a particular business application goes through a series of trust hurdles, with riskier applications requiring more security so that users don't necessarily even know that their logins are being vetted more carefully. Moreover, this all happens in real time, just like the typical multifactor methods. These newer methods include examining your role, or your location, or particular transaction patterns or activities.

Conclusion

Gen Y is pushing the evolution of technology, and with that, the evolution of authentication. With an insatiable desire for anytime, anywhere access to, well… everything, they are demanding easier and safer ways to authenticate – ways that are more integrated, less cumbersome, and of course, more secure, so they can keep their identities, data, and digital lives protected.

With the latest developments in authentication, we may still have to deal with long lines at the coffee shop, but at least our data won't be at risk. And we can have something cool to show our friends that is actually protecting our data in ways we never thought possible.

About the Author

David Strom (@dstrom, strominator.com) is one of the leading experts on network and Internet technologies and has written and spoken extensively on topics such as VOIP, convergence, email, cloud computing, network security, Internet applications, wireless and Web services for more than 25 years. He has had several editorial management positions for both print and online properties in the enthusiast, gaming, IT, network, channel, and electronics industries, including the editor-in-chief of Network Computing print, DigitalLanding.com, and Tom's Hardware.com. He began his career working in varying roles in end-user computing in the IT industry. He has a Masters of Science, Operations Research degree from Stanford University, and a BS from Union College.

About VASCO

VASCO is the world leader in providing two-factor authentication and digital signature solutions to financial institutions. More than half of the Top 100 global banks rely on VASCO solutions to enhance security, protect mobile applications and meet regulatory requirements. VASCO also secures access to data and applications in the cloud, and provides tools for application developers to easily integrate security functions into their web-based and mobile applications. VASCO enables more than 10,000 customers in 100 countries to secure access, manage identities, verify transactions, and protect assets across financial, enterprise, E-commerce, government and healthcare markets.

Learn more about VASCO at www.vasco.com or visit blog.vasco.com


VASCO
THE AUTHENTICATION COMPANY