

Simple passwords have been around for a long time but are now destined to become a thing of the past. Widely recognized as the weakest link in computer security, corporate enterprises and financial institutions are scrambling to find suitable, secure alternatives. This is spurred by the 2005 FFIEC Security Guidance that wants all online financial services to have increased authentication security technologies in place by 2007.

Will Online Users Log On or Check Out

There are dozens of security authentication methodologies to choose from. As organizations select and implement individual solutions, the overall impact on the online community will be substantial. Since the average user has 5 plus passwords, and each organization will adapt their own technology, users will be confronted with learning and using several logon systems.

Power internet users have an even bigger problem. Imagine for a moment a power Internet user with dozens of password protected accounts. These might include: e-Bay, PayPal, an online brokerage account, one or more online banking accounts, one or more e-mail accounts, and several online shopping accounts. Each will have their own authentication technology ranging from tokens, to authenticators, to cryptographies.

The Nightmare Logon Scenario of the Future



Each time a user logs on to a different account, they will need to use a different authentication method. In a world where users already find passwords difficult to remember, the problems created by this scenario are almost insurmountable and will not be tolerated by the end user.

The problem is that while financial services and other organizations are doing their best to address individual authentication security, too many decisions are being made without considering other factors impacting their online user community. They see the problem in one dimension-to provide secure online transactions for their users. Unfortunately, that only solves one problem for one financial institution while creating numerous problems for their customers.

Thousands of organizations will be implementing their own individual solutions. Organizations that create solutions without taking this into consideration will find themselves dealing with everything from increased help desk calls to serious customer relations issues.

Security Only Works If People Use It

For decades we have been bombarded with simple security steps we can take to protect our homes and valuables. For example, we've been told to install deadbolts on our doors at home. So we do it. But do you lock your deadbolt every time you leave your home?

The challenges in the world of online security go beyond that. If the total of online businesses equips the user community with tokens, decoders, and similar authentication devices, users could simply stop using the online services. It will become too difficult to conduct business online and end users will look for new vendors with better security solutions.

Computer tokens are a case in point. One bank equipping customers with tokens for secure online access may not only work, it is actually a novelty that many users might initially find attractive. But the novelty quickly wears off when a second and third token arrive in the mail from other online companies. If tokens become a widely accepted solution, users could easily have as many as 5 or 6 to carry with them for uninhibited, universal access to accounts. Frankly, that's just not going to happen.

More likely than not, the tokens will wind up at home or at work in a desk drawer, lost or even stolen. It's a catch 22. Create tighter security to encourage online use. Online use goes down because the security solution offered becomes a bigger and more visible problem than security breaches ever were.

I Think You're Gonna Need a Bigger Key Chain



Other alternatives such as authenticators and decoder cards create an entirely different set of user issues. By themselves and as a single solution they may work. But thrown in the mix with tokens and other authentication methodologies users are simply being given way too much to deal with.



Electronic Authenticator



Ovaltine Secret Decoder Ring

Electronic authenticators have users correlating passwords to other characters to create a coded password. This methodology is much like that used with the Ovaltine decoder ring offered in the fifties and made

famous again in the movie the Christmas Story. It's hard to imagine users carrying around decoder cards or bringing up electronic decoders on their computer screens to enter a password for multiple accounts.

A Different Point of View

Businesses and financial institutions need to take a serious look at their authentication strategies from a different point of view. Currently authentication evaluations have a heavy slant toward technology and today's user. But it is tomorrow's user that needs to be considered. For example, will tomorrow's user tolerate 3 separate tokens, a decoder card, and a smart card as the paraphernalia they require to simply log on to their accounts?

In the future it is likely that the type and usability of authentication becomes a differentiator in determining with whom to do online financial transactions. Consider the introduction of any new computer technology. Early in the product life cycle it is technology and performance that drives the early adapters to accept a product. But as the lifecycle shifts to the mainstream market, technology gives way to convenience and service. Geoffrey A. Moore calls it "*Crossing the Chasm*". Good technology that never made it includes OS2 and ISDN.

Strong authentication security must be effective and efficient. It must meet the following needs:

- Validates the actual user, not a token or hardware
- Minimum impact on help desk
- Can't be guessed, copied or stolen
- Low cost

But there are important considerations beyond security that determine if a chosen authentication technology meets user requirements in the mainstream market. They include:

- Doesn't take up wallet, key chain, or desk space
- Intuitive and easy to use
- Positive end user experience
- With you wherever you go
- Totally reliable

How Do Current Technologies Stack Up in the Mainstream Market?

Tokens, smart cards, and decoders require users to carry around yet another form of identification that can be lost or stolen. And since most users deal with multiple online businesses and institutions, we are talking about multiple items. More important, these methodologies verify the item, not the user. So if one is stolen or lost, account information can be compromised.

Any solution that requires hardware, like tokens and biometrics, is simply too costly to implement. Not only are there high initial costs associated with buying the hardware and implementation, there are ongoing maintenance and support expenses. Lost or broken hardware must be replaced. But even more important, users with broken authentication devices can't access their accounts. Hardware must be replaced or repaired immediately and this burden will involve and affect the end user.

Software authentication solutions require programs to be loaded on your computer. The technology is with you wherever you go as long as you take your computer with you. This is not an acceptable alternative for most end users today. Technology should be designed to make life easier, not more difficult.

Security is Always about the User

How much of your evaluation process has centered on technology rather than the customer base? If you are like many companies evaluating authentication products, the answer is very little. For most organizations authentication technology is an IT decision based primarily on technology and implementation cost. There are a number of other considerations that are equally if not more important. You must have a good understanding of your customer's online needs and challenges. Otherwise you will develop a security solution that no one uses. Ask yourself these questions:

1. How many total companies will offer or mandate strong authentication to your customers?

Within the next 2 years, most online users will be required to have strong authentication from: banks, credit unions, online brokerage firms, and a number of high profile online shopping sites.

2. How many different kinds of authentication will your customers have to deal with?

End users will have to learn how to use at least two or more technologies.

3. What are the true costs of authentication technologies under consideration?

Aside from implementation, you need to consider, training, customer targeted marketing, call center needs, and maintenance costs.

4. Do you know what your major competitors are offering or intend to offer?

Companies offering a secure, convenient, service oriented solution could gain a significant competitive advantage.

5. How likely are your customers to choose your solution over that of a competitor?

Customers will most likely be forced to choose. At no time in the computer industry has the user base voluntarily or otherwise adapted to and used several competing technologies at the same time.

6. What is the ideal solution from a user's perspective?

Most users would agree that they like things just the way they are with one exception; they believe it's important to be more secure. But what price are they willing to pay for that security? Human nature is such that until their personal security is compromised they will opt to do nothing. Therefore the ideal solution needs to be unobtrusive, require no technical ability whatsoever, and as close to the processes they are using today as possible.

There is one last point. Whatever solution you choose must be visible to the end user. Saying you have made their authentication process more secure doesn't make it so in a user's mind. The perception of stronger security is just as important as the reality.

What's the Answer?

The ideal solution to strong authentication is built primarily around two factors: End User Requirements and Effective Security. Almost all the solutions available today offer the later. Few meet overall needs of the online user community. Assuming effective security, the ideal solution must meet the following criteria:

- **No Hardware Required** – It is unreasonable to assume that users will embrace the idea of carrying multiple tokens with them everywhere they go. Nor will the average user feel comfortable adding hardware such as smart card readers or biometrics to their systems.
- **No Software Required** – Installing software from a single online service provider may be viable. But having to install several types of software from various vendors will not fly with end users.
- **Allows Access On Any Computer, Anywhere** – The online community uses multiple systems. People access online accounts from home, work, and internet cafes.
- **Nothing to Carry, Loose, or Forget** – Using decoder cards or similar items gives users just one more thing to loose or forget. And when the card is lost or stolen, so can their online account information.
- **Simple and Easy to Use** – Solutions can in no way be technical in nature. As digital as the world has become, most people are not technical. The ideal solution is based on something they already know or do, and is not overwhelmingly technical.

One such technology that meets these requirements is Passfaces. This patented technology leverages the mind's innate ability to recognize faces. End users don't need to carry anything, install anything or learn anything to use this innovative technology. By simply recognizing assigned faces, end users can easily and securely log on to password protected accounts from any machine from any location. Both formal and informal studies conclude that people like using Passfaces while providing the strong user authentication required by the FFIEC Guidance.