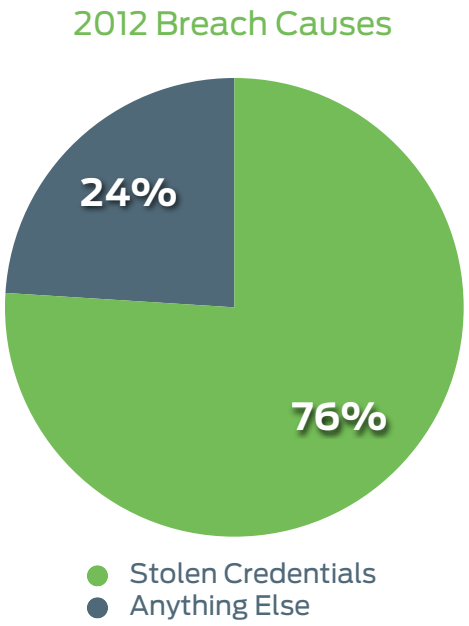
Modern two-factor authentication:

Easy. Affordable. Secure.

www.duosecurity.com

Your systems and users are under attack like never before

The last few years have seen an unprecedented number of attacks on businesses of every size and scope — from community theaters and dentist offices to major social networks and defense contractors. Whether you are trying to protect your remote access or online customer accounts, user ID and password theft is a problem that can't be ignored. Determined criminal organizations, often backed by international organized crime, are out to steal your trade secrets, customer information, and hijack your computers.



Passwords: An attacker's favorite door into your privileged information

Determined criminal organizations, often backed by international organized crime, are out to steal your trade secrets, customer information, and hijack your computers.

Login credentials are the soft underbelly of digital security. Over 76% of the breaches analyzed in the Verizon Breach Report 2012 involved weak or stolen login credentials[1]. By simply obtaining one of your user's login credentials, cyber criminals can remotely access bank accounts, sensitive patient databases, and internal corporate networks. While they're at it they'll wreck your company's good name — and your reputation.

The value of credentials in enabling malicious activity has skyrocketed, and criminal organizations are regularly conducting so-called untargeted attacks. These attacks don't target any particular organization; instead, a criminal organization will send an indiscriminate phishing email or website to find as many credentials as possible.

To make things worse, it is easier than ever to steal user IDs and passwords and use them to remotely access sensitive corporate and customer accounts. Where attacks were once difficult to carry out and were mounted only on "high value" targets, criminals are now targeting businesses of all sizes. Stealing credentials is now as simple as spamming thousands of users with innocuous looking emails containing seemingly familiar links that, when clicked on, install spyware that records keystrokes, including login information. All it takes is one unwary user and your system is open to compromise and takeover. In fact, in 2012, Kaspersky Lab recorded 200,000 new malicious programs every day[2].

Two-factor authentication stops attackers from gaining easy access with stolen credentials

Two-factor authentication stops easy access with stolen credentials by requiring a second level of authentication after the user enters their username and password.

When Zappos, LinkedIn, eHarmony, and Yahoo were breached last year, cyber criminals made off with more than 32 million passwords — and every one of them would be rendered valueless with the use of two-factor authentication. Two-factor authentication stops easy access with stolen credentials by requiring a second level of authentication after the user enters their username and password. Since a password is something that a user **knows**, ensuring that the user also needs to **have** something in order to log in thwarts attackers that steal or gain access to passwords.

This second factor of authentication can take many forms: traditional tokens or key fobs that display a random numerical code, smart cards, texts or alerts on your smartphone, and even biometrics like fingerprint pads.

Traditional barriers to wide-scale two-factor authentication adoption

Unfortunately, adoption of two-factor authentication still runs into resistance. Three primary barriers prevent or slow down the adoption of two-factor authentication: Cost, user experience, and complicated deployment.

High Cost

For many companies the cost of most two-factor solutions remains a barrier. When considering a traditional hardware token solution, the cost of just one token can be more than $100 per user. Then you have to take into account that tokens will often have to be replaced due to loss, theft, damage or malfunction. In addition, this

expense doesn't include support costs, deployment costs, or the fact that tokens need to be replaced every three years.

Poor User Experience

When considering a traditional hardware token solution, the cost of just one token can be more than $100 per user.

A poor user experience both for users and administrators can also be a significant barrier in the way of adopting the higher security of two-factor authentication. With many two-factor providers relying on outdated technology invented in the 1980's (with user interfaces to match), it's no wonder that many two-factor deployments end up being equally hated by both users and administrators.

Complicated Deployment/Installation

Implementing a two-factor solution typically requires dedicated hardware and software on site, ongoing maintenance and administration, and distribution and management of tokens to their users or customers. These requirements not only increase upfront capital investments, but also impact the overall total cost of ownership. Additionally, IT administrators often find their hands full with support requests and complaints after rolling out a token-based two-factor solution. Because individuals don't like being required to carry a token to access their important accounts, many companies end up utilizing two-factor only where required by government regulations (if at all).

Modern Two-Factor Authentication Breaks Down the Barriers

Fortunately, two technology trends over the past few years have enabled a new generation of two-factor authentication solutions that break down these barriers. First, the availability and use of smartphones has exploded — Deloitte predicts that over 1 billion new smartphones will ship worldwide in 2013, with a global base of more than 2 billion smartphone users[3]. Most people don't leave the house without

their smartphone, so it makes a perfect way to prove the second factor of authentication.

Using a smartphone for the second factor of authentication provides a higher level of security. Unlike traditional key fob tokens, users know immediately when their phone is stolen and can take quick steps to eliminate their stolen phone as a valid second factor. Mobile two-factor solutions can also alert the user immediately when an unauthorized login attempt is attempted. Mobile two-factor authentication is also easier to deploy, administer, and use, since users are already familiar with the interface of a smartphone app. Further, some services even offer the convenience of user self enrollment, which results in far quicker deployment with fewer calls to the help desk.

The second technology trend that has led to a new generation of two-factor solutions: The rapid adoption of cloud computing and services delivered through the cloud. Cloud computing allows businesses to rapidly deploy new services without heavy investment in setup and configuration. Moreover, cloud computing simplifies management, as all operational concerns such as backup, security, and scaling are the responsibility of the service provider.

Conclusion

Leveraging consumers' mobile devices for strong, easy-to-use, risk-adaptive secondary authentication, Duo's cloud-based security service requires virtually no end-user configuration

With more and more users accessing their sensitive corporate accounts online, organizations are struggling to keep their sensitive information safe.

Two-factor authentication provides proven protection in a world of increasing threats. But it can be hard to get organizations to buy into traditional two-factor solutions because of high costs, bad user/administrator experience and overly complicated deployment and installation.

Modern mobile based two-factor authentication overcomes these barriers by taking advantage of the wide adoption of both mobile technology and cloud computing. Mobile technology allows for easier use and implementation, while eliminating the need for costly tokens. Cloud computing simplifies management and allows

companies to adopt the security of two-factor authentication without the investing in setup or configuration.

About Duo Security

Duo Security provides cost-effective, scalable two-factor authentication as a service. Leveraging consumers' mobile devices for strong, easy-to-use, risk-adaptive secondary authentication, Duo's cloud-based security service requires virtually no end-user configuration, no hardware installation at the customer site, and includes an easily used web interface for management of user credentials. Duo's two-factor authentication uses a mobile device or phone as a second factor to make integrations simple and the user experience flexible and pain-free.

More Information

Visit our website at duosecurity.com, or speak with a product specialist: 1 (855) 386-2884

Headquarters
617 Detroit Street
Ann Arbor, MI 48104
1 (855) 386-2884
info@duosecurity.com

1: Verizon 2013 Data Breach Investigations Report

2: "*2012 by the numbers: Kaspersky Lab now detects 200,000 new malicious programs every day*", Kaspersky Labs, http://www.kaspersky.com/about/news/virus/2012/2012_by_the_numbers_Kaspersky_Lab_now_detects_200000_new_malicious_programs_every_day

3: "*Smartphone shipments to top 1 billion in 2013*", BGR, http://bgr.com/2013/01/16/smartphone-shipments-2013-estimates-293449/