

maverick™

2-Factor Authentication Scenario* EDUCATION



*Scenario is for illustrative purposes only.
This is not a case study.



maverick™

TOLL FREE / 888-266-1678 WEB / www.MaverickSecure.com

Hello and thank you for your interest in Maverick Secure.

In establishing Maverick I had a vision to build a company that everyone could be proud to work for, be associated with, and would want to conduct business. I believe we have achieved that goal and continue to aspire everyday to make that an on-going reality of continuous improvement. Here at Maverick Secure we are building a company that is run with integrity. Our ethos: SECURITY IS EVERYTHING. Our products, our service, and our mission will not be compromised. Our mission is to provide the most secure authentication process available on the market, and match that with the most affordable price point in the market.

The Maverick family is founded on several core principles:

- To stay ahead of hackers and rogue elements by providing the strongest, most secure, highly innovative and patented authentication processes available;
- To provide a great product at a reasonable price;
- To be responsible to our customers: your success is our success;
- To be responsible to our employees: we all work hard and so we should all share in our collective successes.
- To be responsible to this land that we all share: make every effort to create a sustainable product that will contribute to the health, vitality and industry of this planet;
- To invest in solutions that will enable the business community to grow and develop: businesses of all sizes are the backbone of our communities, our culture and our country.

Maverick Secure is fully invested in developing and protecting a work environment that rewards integrity and embraces diversity. We believe in quality service and support this with a strong work ethic. Here at Maverick Secure, we will not compromise integrity for profit. We will not discriminate on the basis of race, ethnicity, religious preference, sexual orientation or gender – rather, we will truly endeavor to embrace and elevate individuals who deliver on our core values. It's simple really: your success is our success. We believe in good honest work, and we will work hard to produce the tools, the solutions, and resources that make your task easier, more efficient, more profitable and most importantly, MORE SECURE.

On behalf of the Maverick family, I welcome you to learn more about our family of products, and to become our next Maverick Secure satisfied customer.

Thank you.

Patrick McNicholas
Managing Partner



Contents

Education Scenario	1
Welcome	2
Contents	3
Abstract	4
Overview	4
Case Scenario	5
Key Requirements of School	5
2-Factor Authentication Solution	6
Benefits	6
Work, Life Balance	6
About Maverick	7

Abstract

Educational institutions collect, maintain and store volumes of sensitive information and have the responsibility, under the (FERPA), to manage the risks associated with student records and profile information at all levels.

Overview

Increasingly sophisticated malicious network attacks spare no organization connected to a computer network, especially the Internet, Extranet, LAN or WAN.

Case Scenario

A prestigious U.K. primary school successfully achieved a secure solution to the problem of providing remote access to its network and online resources for staff who were essentially mobile.

Key Requirements

The school wanted its teaching and support staff to be able to easily access the school network and other online resources as securely as possible from the comfort of their homes or from any location they currently chose to work in.

2-Factor Authentication Solution

School identified Maverick's 2-F strong authentication solution as the best one that met their requirements.

Benefits

The solution was elegantly simple. School staff only had to insert their authentication key into their home or laptop computers' USB port and the key generated an OTP (One time Password).

Work, Life Balance for School staff

Staff and teachers appreciated the convenience the secure VPN + Authentication Key solution provided for them.

About Maverick

Teachers were quickly able to share the day's agendas, lesson plans and best practices and review student materials from their home computers. It also had the following advantages:

- Reduced risks.
- Sensitive data was adequately protected.
- Allowed deployment of simpler, user- friendly but totally secure policies for network access.

Vulnerable school network services include:

- Remote access by staff (especially those in management positions) to school networks.
- Parental access to their children's grades and other records.
- Web portals for use by pupils and teachers.
- Applications hosted at school servers and government institutions.
- Remote desktop access through Virtual Private Networks.

Without secure authentication and preventive systems in place, these services can be compromised by a skilled hacker.



Abstract

Educational institutions collect, maintain and store volumes of sensitive information and have a responsibility, under the "The Family Educational Rights and Privacy Act" (FERPA), to manage the risks associated with student records and profile information at all levels. More importantly, the school's online portals and web-based resources that are remotely accessed by students using their laptops, tablets, smartphones, iPhones or iPads are extremely vulnerable to security breaches and cyber attacks. Therefore, it is imperative that this information is protected by proper means of security and authentication. Maverick Secure LLC's new product, Maverick 2-FTM enables education universities/agencies of all sizes to secure access to their confidential data and critical systems by adding two-factor authentication, also called strong authentication. Two-factor authentication reduces the window of opportunity for fraudsters and can eliminate, contain or mitigate online attacks. Implementing and rolling out a two-factor authentication solution to a large user base involves a significant investment. As such, it is important to have a good understanding of the benefits and limitations of two-factor authentication technologies and the relative strengths and weaknesses of devices and solutions, before making a decision.

Overview

Increasingly sophisticated malicious network attacks spare no organization connected to a computer network, especially the Internet, Extranet, LAN or WAN. As more and more schools connect to the Internet to improve and enhance their services, they are vulnerable to malicious attacks if they don't have a strong security system in place. Few school administrators are aware of the real scale of the security risks posed by unsecured school computer networks as a lot of school information can be compromised without secure precautions in a school network environment. Confidential information such as test results, student and teacher performance reports, salary information and deductions, teacher loans, school medical records and other sensitive school information are vulnerable to being accessed or worse, modified or deleted by malicious parties. There are even possibilities of inserting new fraudulent data for a whole series of malicious intentions.

At-A-Glance

Key Requirements of School

Full network and remote desktop access by staff to school network through VPN connectivity. Two-factor authentication that required no keying in. Solution needed to be easy for students and teachers to use. Should be cost effective and within budget. Should allow secure access to third party systems or networks.

Two factor Authentication solution

Zero-installation 2-factor Authentication Key to establish a secure VPN connection. Allowed auto-typing of one-time passwords (OTP)

Benefits from 2F Authentication Implementation Solution

Teachers were quickly able to share the day's agendas, lesson plans and best practices and review student materials from their home computers. Reduced risks; sensitive data were protected. Allowed deployment of simpler and more user-friendly policies for network access.

Those with harmful intent are not limited to outsiders. Current and former employees and students, even officials (for various reasons) now have the potential to be a school cyber-attacker, thanks to the wide availability of hacking information over the Internet. Anybody with a grudge or curiosity now has the means to cause electronic harm to schools, teachers, and students alike. Recovering from, and investigating, school network breaches can lead to loss of time and resources that are better devoted to teaching. It also creates a school atmosphere steeped in suspicion, and promotes lack of confidence in authorities and the systems in place. It's not just schools that are at risk from security breaches. Even the biggest of data and security companies, in spite of their advanced security technologies, can still be vulnerable to malicious network attacks. The risk level is compounded hundredfold at schools with no safe computing policies and secure systems in place.

Some examples:

- Even Google had problems with a security breach in China in 2010.
- In early 2011, a leading corporate security provider was hacked.
- Recently the FBI and U.S. Justice Department web sites were crashed by hackers in apparent retaliation for the taking down of a popular file-sharing site.

Case Scenario

A prestigious U.K. primary school successfully achieved a secure solution to the problem of providing remote access to its network and online resources for staff at home and mobile.

Key requirements of School

The school wanted its teaching and support staff to be able to easily access the school network and other online resources as securely as possible from the comfort of their homes or were in multi locational access mode. They determined that the acceptable level of security would be best accomplished through remote desktop sharing remote users who would be able to run an instance of their school desktops from the comfort of their home or laptop computers, or access the school's LAN as if they are just in the school premises.

But the school had no control over the security systems on the home PCs, laptops, and other computers the school's staff would be using to connect to the school's network putting the users and the network at risk to malware and hacker sponsored activities. The IT staff saw that the solution required encrypted network sessions plus a strong authentication method that was not vulnerable to network sniffing. Plus, the solution had to be simple, easy to use, and should fit within the school's tight budget.

Two-Factor Authentication Solution

The school's tight budget quickly ruled out several other solution vendors and their offerings. Finally, the school IT committee settled on a major network security service provider who offered a combination VPN (virtual private network) plus Authentication Key (for two-factor authentication) solution which fitted the school's IT security and remote networking requirements and its budget. The school tested the chosen solution first on a pilot group of five administrators, then, after weeks of testing, rolled out the solution to the rest of the teaching and support staff.

Benefits from two factor authentication to school

The solution was elegantly simple. School staff only had to insert their authentication key into their home or laptop computer's USB port and the key generated an OTP (one-time password) that was automatically entered onto the school network's login screen with just a touch of the key's button which meant there was no need to install anything. Plus, the design allowed the school to simplify their policies for accessing the school network within the premises or even externally. This enabled the teachers to do their school networking tasks from their home computers without worries sharing agendas, lesson plans, and best practices with other members of staff; and allowed reviewing student materials while saving documents and other materials directly into the school's server. Thanks to VPN connectivity, the teachers were also able to remotely print their materials from their home computers directly to the school's printers, greatly enhancing their productivity.

Work, Life Balance for School staff

Staff and teachers appreciated the convenience the secure VPN + Authentication Key solution did provided for them. It required less of their active time, required little maintenance, and they no longer needed to carry their laptops between home and school, plus, they could work practically anywhere there was an Internet connection without worrying about network security. This allowed them to focus on what they need to concentrate on: educating children. The network solution also helped streamline the school's application to become an academy by allowing the teachers to submit their requirements online. To date, the IT and teaching staff had encountered no issues with their chosen two-factor authentication solution. Users thought it had been a perfect fit with their needs so far.

About Maverick Secure LLC

Maverick provides multi-factor authentication solutions to safeguard confidential digital records and data. It is applicable to industries including technology, Internet, healthcare, education, financial services, government, military and subscription services. Maverick's strong multi-factor authentication processes are your solution when passwords just aren't enough to protect your sensitive data from unauthorized users and hackers.

The Maverick brand is dedicated to providing the business community with a high quality and affordable alternative to the pre-existing/overpriced offerings currently available in the market. By providing user-friendly, scalable and seamless compatible technologies, our products match and very often exceed our competitors' products while remaining price sensitive, affordable and much greater offering value for money.

Maverick offers stronger security by leveraging the industry's leading multi-factor authentication processes in very unique and efficient out-of-band channel methods. By living up to its name, Maverick takes a unique "out of the box" strategic perspective in protecting our clients from the threats that surround us in this constantly evolving security-vulnerable world. Maverick provides an easy-to-use approach for users while providing the highest level of security as an overlay to existing business applications and systems.

The Maverick brand started out as Maverick Computers and was named as "One of the fastest growing computer companies in North America," "#1 Solution Provider" and the "#1 System Builder in North America based on growth (2004)," and "Server Innovation Award" by CRN Magazine for developing a virtually indestructible server. The company then launched a new sister company called Maverick Communications which was awarded "2005 North American System Builder Association – Business Innovation of the Year" for creating an integrated array of video, voice and data services that included what was then the world's fastest Internet access for consumers at 45mbps. Over the past five years a new division of the Maverick brand, Maverick Secure LLC., was launched to combat the ever-evolving and tenacious attacks of hackers such unauthorized access of data and the multitude of other security breaches have caused serious turmoil within the computer and associated industries. In 2009 Maverick partnered with IBM, the number one server company in the world for enterprise users, to develop the "Maverick SMART Server Powered by IBM." By utilizing the award winning hardware of Maverick Computers, the industry's leading authentication process of Maverick Secure and the online and business applications of IBM, Maverick is now positioned to deliver end-to-end solutions for businesses small and large. We believe we have brought together the perfect harmony of leading technologies to offer one of the most secure solutions that addresses issues related to password authentication.

Contact Us

To learn more about how 2-Factor Authentication products, services, and solutions help solve your business and IT challenges please contact your local representative or authorized reseller.

Patrick McNicholas

President

Maverick Secure, LLC.

Patrick@MaverickSecure.com

www.MaverickSecure.com

772-216-9535 (Cell)

888-266-1678 (Toll-Free)

305-600-0772 (Miami)

917-470-9469 (New York)

415-424-4245 (San Francisco)

020-337-174-11 (London)

888-219-0113 (Fax)

GoToMaverick (SKYPE)

Maverick helps organizations secure and manage their information-driven world with security management, endpoint security, messaging security, and application security solutions.

Copyright © 2012 MaverickSecure.com
All rights reserved.