A Nooch, Inc. White Paper

3 Scarlet Oak Dr.
Haverford, PA 19041
(610) 229-9001
www.nooch.com

Mobile Security:

Protecting Your Money in a 21st Century Environment

By Cliff Canan | *President*
cliff@nooch.com

June 22, 2011

Contents

Introduction

21st century threats are challenging businesses every day, requiring new investment in technology and renewed dedication to training, education and prevention.

Problem Statement

With hackers getting smarter every day, financial firms must stay on the cutting edge of technology and security to protect their customers' sensitive personal information.

Nooch Solution

Nooch is taking a proactive and comprehensive approach to ensuring that users' information is secure and protected.

Evolve IP – Strategic Partnership

Nooch has partnered with Evolve IP, an industry leading technology firm with an expert team of specialists and an unparalleled track record.

Exceeding Federal Compliance Standards

Nooch is committed to going far beyond what is required by law to keep personal data secure. PCI, PA-DSS, VeriSign, and other software protocols are in place to minimize risk.

Unique Verification Features

Nooch uses geo-location, the power of social networks and device-linked accounts to maximize user protection and peace of mind.

Summary

Nooch's commitment to security is a never-ending effort as we continually invest in the next generation of technology and innovation.

I. Introduction

In today's world of sophisticated 21st century technology, the opportunity for predators, hackers and other digital criminals is enormous. More and more US consumers are conducting their daily business online, exposing themselves to the costly consequences of losing control over their most sensitive personal information. The costs to business and consumers alike can be staggering: companies around the globe lost $1 trillion from data loss in 2008 alone.[1] The average company suffered $1.2 million in losses.

Every single day, consumers enter their private information like their address, credit card numbers, phone numbers and even their social security numbers in order to shop online, apply for a new credit card or get a new social networking account. With every submission, consumers risk having that information exposed to people who can wreak havoc on their lives, taking a potentially huge financial and emotional toll.

Words like "malware," "phishing," "spyware," and "data breach" have become all too common on nightly news shows. Companies big and small, local and global, financial and retail are all vulnerable to security attacks. In the health care industry alone, there were over 225 breaches of more than six million patient records just since August 2009. 61% of these breaches were the result of malicious intent.[2]

As more and more companies begin to store their data in the cloud, cybercriminals have developed new ways to target this information. According to a 2011 McAfee report, *"The cyber underground economy has shifted its focus to the theft of corporate intellectual capital–the new currency of cybercrime."* [3] Hackers are realizing the immense value of the corporate data minefields that are stored on virtual servers. Even the most sophisticated corporations like Sony, Google, ExxonMobil and Bank of America (not to mention the US government itself) have been subjected to damaging cyber attacks.

As the bad guys get smarter, companies in all industries must make data security a top priority if they are to survive in the 21st century economy. This new world is composed of primarily intellectual capital that provides ripe new opportunities for creative cybercriminals. More information than ever is shared via e-mail, cloud-based servers and other modes of communication that offer just as much potential for theft as they do convenience, efficiency and speed for the companies who use them every day.

And with the newfound prominence of organizations like Wikileaks, companies around the world are now forced to deal with the most difficult threat of all: insiders who deliberately spread or sell proprietary information for their own purposes. All the technology in the world cannot stop a disgruntled employee with enough access from exposing thousands of consumer profiles, financial information, legal documents and more. Every company who cares about its customers and its own ability to survive must examine its existing security protocols and evaluate whether it is utilizing the most sophisticated systems available to prevent data loss.

---

[1] *Underground Economies.* McAfee Report. 2011
[2] *Breach Report 2010: Protected Health Information*. Redspin. 2010.
[3] *Underground Economies.*

To be sure, the incentives for cybercriminals to develop the next great attack are stronger than ever and are not going away. In 2010, Gordon Snow, Assistant Director of the FBI testified before House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security:

> "The impact of cyber crime on individuals and commerce can be substantial, with the consequences ranging from a mere inconvenience to financial ruin. The potential for considerable profits is enticing to young criminals, and has resulted in the creation of a large underground economy known as the cyber underground… a pervasive market governed by rules and logic that closely mimic those of the legitimate business world, including a unique language, a set of expectations about its members' conduct, and a system of stratification based on knowledge and skill, activities, and reputation."[4]

Financial firms in particular – since they offer the most direct access to consumers' bank accounts and other valuable data – must stay vigilant in the fight against cybercrime. They need up-to-date policies in place to train and educate their employees and their customers. But more important, these firms must ensure that they are constantly investing in the technology solutions of tomorrow in order to mitigate these threats before they fall victim to costly data breaches. Whenever money is involved, as with banking transactions or any transfer of cash, criminals will do whatever it takes to crack the corporate code and steal valuable data.

Consumers' wariness of cyber theft has been intensified by the many high-profile episodes of expensive attacks on companies like PayPal, Visa and MasterCard. While a new generation of adults has been raised to trust the internet and often provides their precious information with nary a second thought, the need for vigilance is still high. Consumers expect – rightly so – that the businesses they choose to trust with their data are doing everything in their power to protect that information. They expect companies to go beyond the bare minimum required by law. They expect honest communication about attacks, immediate remediation whenever fraud or theft occurs and above all, they expect that businesses care as much about their data as they do.

And, of course, the increasing trend towards mobile commerce presents another set of challenges for today's companies. There are more end-points than ever which all present fresh opportunities for the theft of confidential information. New devices, various smartphone designs, and social networks allow consumers to be more connected than ever before, resulting in unprecedented gains in workplace efficiency. But along with the incredible new ability to communicate and collaborate, consumers face the added prospects of much increased risk that their data could be leaked. Companies can never remain complacent as cybercriminals are constantly evolving their own methods of attack.

The good news, however, is that smart companies who recognize the threats that are out there have an advantage. While no system, policy or single technology can ever guarantee total security, today's businesses are implementing a wide range of measures that can minimize the risk that they and their customers face. With proper planning, sufficient dedication to investment and education and a business culture that welcomes new technology with openness and honesty, companies can take their cyber-security into their own hands.

[4] *Underground Economies.* McAfee Report. 2011

II. Problem Statement

Today's cybercriminals are using the sophisticated new technologies to exploit every potential vulnerability in corporate America's infrastructure, human network and data storage systems. These tactics can include:

Attacks on Software:

- Denial-of-Service (DoS) attacks
  - distributed denial-of-service (DDoS)
  - Permanent denial-of-service (PDoS)
  - Smurf attacks
  - Ping floods
- Trojan attacks
- Viruses, malware and spyware
- Cyber espionage
- Penetration attacks

Attacks on Hardware:

- BOTS that take over computers and servers
- Wireless network exploitation
- Password crackers like key loggers
- Hardware theft
- Smartphone attacks

Attacks on People:

- Social engineering
- Phishing scams
- Social network attacks[5]
- Extortion and blackmail

[5] http://arxiv.org/PS_cache/arxiv/pdf/1010/1010.1028v1.pdf

III. How Nooch is Fighting Back

Nooch is committed to ensuring that all of its users experience a hassle-free experience. Part of this commitment includes a dedication to security through technology, education and prevention. Nooch understands that users are taking a leap of faith when they sign up to use Nooch's peer-to-peer money transfer system, and that faith should be rewarded with nothing less than a thorough focus on utilizing the most sophisticated processes available today to make certain all data is secure.

Before even launching, Nooch is investing heavily in building the most robust software possible in order to prevent problems before data is vulnerable. In addition, Nooch is going far above and beyond what is required by federal compliance standards and regulatory schema. In addition to obtaining PCI compliance, establishing strong personnel training programs and maintaining ultra-secure private servers, Nooch is developing industry-leading procedures in order to handle any conceivable conflict, attack or fraud that could affect its system.

Financial data is more valuable to potential criminals than any other type of information. Nooch will always strive to keep its users wholly informed of all security measures the company establishes, while also communicating any would-be threats or attacks we may face. Nooch is a community of people who are tired of being nickel and dimed by impersonal big banks. Our team understands the frustration of corporate secrecy and inept customer service, especially when it is *your* data that could be vulnerable. In keeping with our commitment to always be evaluating our security procedures, we welcome any and all feedback that will help us build the most secure and reliable money transfer system in the world. Our success is totally predicated on the trust and comfort level of our users.

Whether it is the Nooch mobile application, our back-end servers or the team members we bring on board, everything we do begins and ends with secure and reliable service. Nooch is building a different kind of financial company – one that treats every customer, big and small, with respect. Consumers will not and should not give second chances to companies who abuse their trust and are haphazard with their sensitive personal information. That is why Nooch is working tirelessly before launch to ensure we've done everything we possibly can to protect consumers' data.

Here are some of the ways Nooch is securing all information we collect:

Industry Leading Encryption

All data received or transmitted by Nooch will always be under **256-bit encryption** (Advanced Encryption Standard), which is even stronger than what the Federal Government requires for Top Secret documents (192-bit). This encryption will be present within our servers, networks as well as on all Point-to-Point transmissions and end-points, blocking unauthorized access to all sensitive information. This helps prevent cybercriminals from stealing your data when you initiate a transaction from your mobile device or from the Nooch website.

Private, Co-located Servers

Part of Nooch's overall security apparatus includes a strategic partnership with Evolve IP, a leading cloud-based technology firm. Evolve's team of security experts manage all physical hardware associated with Nooch's servers (SAS 70 cert. and PCI Compliant) while providing 24/7 management and monitoring of all Nooch platforms. Evolve maintains world-class infrastructure and cutting-edge technology (including comprehensive database management, dual/redundant fiber rings, active/active platforms and carrier independence)[6] that ensures Nooch is always up to date with the most sophisticated prevention processes. Evolve IP provides a unified and seamless solution for Nooch which allows for the most robust Quality of Service (QoS) available.

PCI & PA-DSS Compliant

All Nooch software is built to comply with all aspects of the Payment Card Industry (PCI) and Payment Application Data Security Standard (PA-DSS) requirements. These requirements pertain to the way Nooch receives, stores and displays all credit card information, including the credit card number, expiration date, cardholder name, magnetic stripe information, PIN and other data. Nooch's secure payment application will minimize the potential for security breaches and the potential of fraud.

VeriSign SSL Certification

The VeriSign Trust Seal assures customers that a site is both secure and trusted. Viewed up to 250 million times a day on over 90,000 Web sites and in 160 countries, the VeriSign seal has become the most recognized trust mark on the Internet. This means that the Nooch website:

- is **secured** with VeriSign SSL, issued by the leading Certificate Authority worldwide
- has passed a **daily malware scan**
- will show a green address bar in high-security browsers to provide a visible sign of security and trust

Enterprise Firewall

Nooch employs a next-generation firewall that blocks the latest threats and eliminates unwanted traffic with global reputation technology, application-level protection, encrypted traffic inspection, intrusion prevention, and content filtering. This scalable solution will allow Nooch to stay protected as we grow.

Anti-Virus Protection

Nooch will maintain advanced anti-virus protection in order to mitigate the threat from malicious content through e-mail, DoS attacks and penetration attacks such as trojans, malware and spyware.

[6] http://www.evolveip.net/technology.asp

Geo-Location

Whenever signing up for Nooch from a mobile device, new users will be prompted to allow geo-location. Smartphones today have a GPS chip inside, and the chip uses satellite data to calculate the user's position. When a GPS signal is unavailable, geo-location apps can use information from cell towers to triangulate a user's approximate position.

Some companies like Foursquare use this data to keep your friends abreast of your location in order to enhance social networks or provide location-specific deals or coupons to local merchants. *Nooch will use this data for security*. If a user signed up for Nooch in California, but Nooch detects the account is being accessed from a device in Florida, Nooch will immediately alert the account owner of the suspicious activity and investigate the transaction. While it is possible that the owner is simply traveling, Nooch's system will raise red flags when it detect possible fraudulent activity order to prevent unauthorized access to our users' accounts.

Device-linked accounts

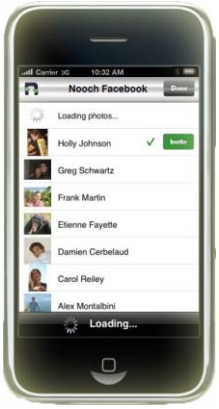
All Nooch users' accounts will be linked to the specific device that the user first used to sign in to their account. This means that if someone steals your account credentials and attempts to log in from their own smartphone, they will be unable to do so. If this happens, Nooch will immediately notify the account owner and investigate. Of course, if users lose their phone or buy a new device, they will be able to easily update their device within Nooch by entering their secure PIN (*see below*) and password.

Unique Nooch PIN

Every Nooch user will be prompted to select a four-digit PIN upon creating their account. This PIN will be required each time the user wants to see their account information like their balance, transaction history or credit card information. The PIN will also be required in order to initiate any transaction. This simple process works just like the PIN debit cards use: if a user's phone is stolen, unauthorized users will not be able to enter the account, see personal information or make any payments.

Picture Confirmation

Because Nooch utilizes the power of Facebook's API, users will see the profile picture of the person they are attempting to send money to before completing the transaction. This will help reduce the risk of accidentally sending the wrong "John Smith" money if users look up your recipient through Facebook. If the recipient is already in a user's "Nooch List" (which would be the case if the user had previously sent that person money through Nooch) or the recipient is in the user's address book, a picture would also be displayed.



Summary

The 21st century business environment provides unprecedented opportunities for collaboration, increasing the efficiency of the worldwide workforce while allowing lightning-fast communication anytime, anywhere. But the blessings of technological advancement come at the cost of continued vigilance against cybercriminals and hackers who see fresh ways to obtain private information. Consumers have come to expect the services they use to maintain the most sophisticated, pro-active measures available in order to safeguard and protect their data. As more and more mobile devices hit the market, consumers are shifting their focus from stationary PCs to the limitless opportunity of constantly being on the go.

This new freedom of movement presents entirely new challenges for companies who chose to develop mobile strategies – especially when they are in the business of handling or transmitting money and financial data. To mitigate the threat from cybercriminals, business must continually invest in the next generation of fraud detection and prevention in order to ensure their customers have the peace of mind they demand.

Nooch is a company that is on the cutting edge of this new revolution in technology and security. Nooch is building on the most successful procedures on today and innovating for tomorrow's new challenges. Working with Evolve IP, an industry leading cloud-based technology firm, Nooch is fully committed to staying attentive to continually improving all of its security processes. In addition to government-grade encryption and full PCI PA-DSS compliance, Nooch is utilizing the latest in mobile technology like geo-location and social networks to mitigate the threats of the new century.

This commitment means heavy investment during the development of Nooch's mobile applications and back-end servers and databases. It means communicating frequently and openly with our partners, regulators and especially our users. While there will never be a single technology or single prevention technique that will eliminate the risk of doing business today, Nooch is following a strategy of always seeking out the best practices for data security. Security is the number one priority at Nooch, as our success is fully dependent on our users' comfort level with relying on Nooch's money transfer system.

Designed for simplicity and convenience, Nooch will never compromise on security for the sake of profit. Instead, Nooch will lead the way by building the world's most reliable way to send money to friends.