



## **Remedies for Phishing and spyware, malware and keyloggers for online banking/financial service providers and merchants.**

---

In 2003, the FTC released a survey showing that 9.9 million American fell victim to identity theft in 2002. Identity theft losses to business and financial institutions totaled \$48 billion; consumers reported \$5 billion in out-of-pocket expenses. The survey also found that 3.23 million consumers discovered that new charge accounts were opened and other frauds had been committed in their name and that 6.5 million victims reported misuse of their credit card accounts.

### ***What is Phishing***

“Phishing” is a spam-based scam that recently has grown in popularity. Phishing is not a cyberattack that propagates malicious code and which is designed to deceive users into doing something that will harm them or their businesses. Phishers send emails that appear to come from a legitimate source. The message often states that there is a problem with the user’s account and requests that the user confirm the merchant’s information by entering sensitive one’s financial information or user credentials into the phisher’s web site that looks exactly like the merchant’s web site. Using this information, the phishers can steal access to the account or perpetrate identity fraud. Phishing also could provide attackers with access to enterprise systems, although it primarily is used for identity theft.

## ***What are the current remedies to prevent Phishing?***

Industry experts provide several suggestions as a means to prevent phishing attacks; however, they heavily emphasize user campaign and education, leaving the first line of defense on each and every end user:

- Educate employees and customers about your e-mail policies.
- Define and communicate consistent enterprise wide policies for contacting users by e-mail.
- Set up an e-mail address (such as spoof@yourcompany.com) and phone number where users can report fraud.
- Immediately notify authorities and customers when you detect a phishing attack, and request that the Internet Service Provider hosting the attacker's site remove it.

Unfortunately, these cannot effectively prevent phishing attacks.

## ***What are the pros and cons of current anti-phishing tools?***

The industry experts including the Gartner Group have identified remedies for anti-Phishing and they are as follow:

- Strong User Authentication via One Time Password (OTP) tokens and/or Public Key Infrastructure (PKI)

*Pros:* This approach is suited for well-defined and relatively static and small communities of participants.

*Cons:* This approach doesn't work well for large volumes of end users. The authentication system should be able to handle a large volume of transactions and the cost of strong authentication should not become a prohibiting factor. Strong authentication means (Smart card, OTP /USB token) prohibits adaptation by the mass public. The PKI is proven to be difficult to deployment and high maintenance costs.

- Shared-Secret Relationship Authentication

*Pros:* The secret is easy for consumers to remember and use. It requires no infrastructure changes by consumers and little implementation effort from the providers.

*Cons:* Shared-secret authentication is device-dependent, and it is subject to "man-in-the-middle" attacks in which phishers or other hackers can trap the shared secret or picture. Keyloggers and malware are becoming more intelligent and will capture user graphics and screen. Deployment of this solution may further instigate the password- reset problems.

- Caller ID for the Internet

*Pros:* This approach is suited for for well known online service providers and its communities of participants.

*Cons:* To enable caller ID for the Internet, Internet browsers must be modified in concert with standards, and consumer browsers would need to be updated or toolbars/plugin downloaded. Legitimate commerce sites would have to pay for higher-security domain name registrations. However, sophisticated phishers still can create "looks legitimate" URLs to allure end users to their phished web sites. Lastly, this solution cannot prevent keyloggers, which are often the causes of New Account Theft.

## ***How StrikeForce Technologies meet the challenge***

The objective of conventional One Time Password (OTP) token is to avoid sending reusable passwords or other secret credentials over the session channel where they can be stolen by keyloggers or other eavesdroppers. This method uses second level of user authentication when users initiate login to their online accounts. However cost of tokens and deployment of a large volume of tokens have been a prohibitive factor for OTP tokens being mass public adoption. Other vendors use SMS text paging for sending OTP over the data channel still pose problems for large adoption in the U.S. due to data network interconnection issues and lack of popularity.

StrikeForce Technologies uses a holistic approach to secure the end user credentials, not only protecting user ID and password, but also protecting all the information a user entering on a keyboard. This approach gives complete end-to-end protection of the user credentials not only being hacked at the network level but also protects from spyware and Trojan horses.

StrikeForce believes that problems of phishing should be addressed in conjunction with keylogging through a holistic approach. Although keylogging and phishing pose a different set of problems and threats to end users, an effective solution should be able to address these at once in coherent manner. For example, when phishing attack is coupled with keyloggers, such impact would be detrimental to end-users even if they were not phished. Thus, we believe that anti-phishing solutions must address the following:

1. Strong Authentication method that leverages consumer appliance as an authentication device – cell phone and phone

StrikeForce uses patent pending technology, ‘Out-of-Band’ authentication. With this method, the users send their authentication credential to the server via the alternate communication channel. This approach works with all phones (although cell phone provides the most convenient user experience). A customer provides his credentials on a login page of his online service providers. The security server then calls the customer’s registered phone number on record and asks him to enter a phrase, password or even biometric voice print/fingerprint on the phone. Successfully completing these steps allows access to the account.

*Benefits:* The most secure way of protecting user credential by splitting a pathway of user information. Suitable for mass public authentication solutions by leveraging existing consumer appliance as an authentication device; no need for special tokens. Eliminated token deployment issues. Providing ability to layer different authentication methods if highest security desired.

2. Encryption of every keystroke at a keyboard

The objective of securing keystroke logging through 128 bit encryption is to protect user data from Trojan horses, spyware and keyloggers.

StrikeForce keystroke encryption technology enables online service providers to extend a SSL encryption channel down to a keyboard level and activates the encryption channel per need basis. While our 128 bits encryption technology is being in effect, any malicious codes or spyware are impossible to hack the user data, because we not only encrypt the data but also send them to a web browser through a different keyboard driver channel (so called Out-of-Band).

The encryption technology is seamlessly integrated into web browsers without rebooting, configuration or manual invocation and termination of the program.

*Benefits:* the most secure way of protecting user credential through 128 bits encryption at a keyboard level which virtually makes impossible for keyloggers, spyware and Trojan horses to hack user data. And the technology seamlessly works with MS Internet Explorer and Netscape browsers. Currently servicing 15+ million online banking and financial service users, ease of installation via inserting a single line of code into a web server. (For more information, see “StrikeForce Technologies Guarded ID™).