

Security For Online Banking That Users Want and Will Pay For

PhoneFactor Study



PhoneFactor, Inc.
7301 West 129th Street
Overland Park, KS 66213
1-877-668-6536
www.phonefactor.com

Conducted By:



Harris Interactive
60 Corporate Woods
Rochester, NY 14623-1457

Introduction

As cases of identity theft rise to unprecedented levels, online banking customers are growing increasingly dependent on their trusted service providers to insulate them from the malicious threats that continue to increase in number and severity. In fact, a study conducted by Symantec noted an increase of 468% in the number of new threats in 2007¹. In addition, more sophisticated threats have emerged recently that are redefining established security best practices.

The most prevalent threats include phishing, keystroke logging, credit card skimming and man-in-the-middle attacks. The magnitude of their infiltration into the financial services sector is astounding. According to Symantec:

- 80% of all unique brands used in phishing attacks were in the financial services sector
- Of all confidential information threats 76% were keystroke logging related and 86% were remote access related
- Bank accounts were the most commonly advertised item for sale on underground economy servers (22% of all items listed)¹

This paper will look at how these threats affect online banking customers, their feelings about the current level of security and willingness to adopt additional security measures. The paper includes the findings of a study conducted by Harris Interactive which was commissioned to understand how a financial institution's customers would perceive the value of PhoneFactor, a unique phone-based authentication solution, by their institution as a value add to their current solution.

Finding A Solution

The industry has already been self-regulating for some time with various security regulations such as FFIEC and PCI. From these regulations, solutions such as security questions, SiteKey, certificates, and tokens have been put into place with various degrees of success. Problems such as user acceptance, user management/support, high cost, and lack of security have all been barriers to wide-spread adoption.

Emerging security concerns such as in-band authentication (using the same communication path that you are logging in on to validate who you are – a problem for man-in-the-middle attacks) defeat many existing two-factor solutions, and none of these solutions take a proactive approach to alerting customers that their credentials have been compromised.

Based on these and other scenarios, PhoneFactor developed our proprietary two-factor authentication solution that solves many of these critical matters.

1. Symantec Internet Security Threat Report: Trends for July–December 08, Volume XIII (April 2008)

Because Passwords Just Aren't Enough

PhoneFactor's two-factor authentication uses an easy process.



Step 1: Login and instantly receive a call.

Step 2: Answer & press # to authenticate.

There are currently 3.5 billion active mobile phone subscriptions today. The security of PhoneFactor lies in its ability to strongly authenticate users based on proof that they know a secret (their password) and are in physical possession of a unique physical device (their phone). While it may be possible (or even easy) for an attacker to gain access to a user's login credentials, it is usually much more difficult to obtain that same user's phone.

Additionally, PhoneFactor provides the security of out-of-band authentication. Because the telephone operates on a totally different communication channel, man-in-the-middle attacks are impossible to deploy. PhoneFactor also stops other password security breaches caused by phishing, keystroke logging and credit card skimming.

PhoneFactor offers a built-in real-time fraud alert. If your phone rings while you are driving down the road, you are likely not accessing your bank account. You know that someone has hacked your password. With PhoneFactor, all you have to do is press ## to freeze your account and instantly alert the bank's fraud department. There are extra levels of security that can be set up in special situations to direct a "bad guy" to a false account so that they think they are continuing the transaction until you make a physical location as well.

For high-risk and high-value transactions, PhoneFactor protects against man-in-the-middle attacks. By providing details about the transaction in the verification call, even if the user's authenticated session has been hijacked, their transactions are protected.

A Case For PhoneFactor

PhoneFactor offers strong, out-of-band authentication, yet is extremely user-friendly. It works with the customer's existing phone (landline or mobile) and can be used to secure account logins, password and other account changes, high-risk transactions and credit card purchases. PhoneFactor is easy to install. It integrates seamlessly with your existing online banking application. There are no

devices to mail or certificates to install, so setup and deployment are quick and easy. No user training is required, and there is very little ongoing user support. Customer acceptance of PhoneFactor continues to grow in every industry.

Financial institutions from the largest on Wall Street to the local on Main Street are adopting this best practice on behalf of their customers and employees with various security options and payment models. As attackers become more sophisticated, customers continue to rely on their service providers to deliver the best options in a competitive marketplace.

The following study indicates that online banking customers are not confident that their financial institutions are taking appropriate measures to ensure the security of their personal data and financial accounts. Financial institutions can leverage PhoneFactor to increase customer loyalty and win new business. Read the full study that follows to learn more.

Survey Overview

In March of 2008, Harris Interactive performed a survey of 1500 respondents online who have engaged in online banking, online stock trading, or have checked credit card balances online. The sampling error on the following data is 2.43%

Consumers Perceive Significant Weakness in Online Banking Safety

Reality doesn't often count; it's perception that counts.

64% of those surveyed felt it was only "somewhat difficult" or "not at all difficult" for a hacker or thief to get access to an online banking account (42% said "somewhat difficult" and 22% said "not at all difficult").

Regardless of current safety measures, and current spending levels towards online banking security, nearly two-thirds of online banking customers think otherwise.

One of Every Three-to- Five Online Banking Customers Would Buy

Purchase intent statistics can be overstated and must be looked at with a progression of questioning. At first, consumers will often say, "Yes, I would be interested" in general terms. This is often called the "novelty effect." We only need to look as far as new products like Pepsi Clear to see historical failures of research combined with a product which can easily be tried but not repeated.

Survey design is such that we see the highest numbers first and then drill down to more specific questions.

Upon first description, 48% said they would be “extremely” or “very” interested in the PhoneFactor service from their bank. 93% indicated some level of interest. Six questions later, the same respondents are asked how likely they would be to sign up for the service with their bank charging a specific price of \$3.95 per month.

With the PhoneFactor service only being used for login access safety, 20% said they would be “extremely” or “very” interested in the service from their bank at \$3.95 per month.

With additional protection of the service (an automatic call in the same manner to approve high-risk or high-dollar transactions like international transfers or transfers in excess of \$5,000) the demand increased substantially. With this additional feature, 31% of all respondents said they would be “extremely” or “very” interested in signing up for the service.

With just login access safety, Top Box scores yield a 20% adoption rate of PhoneFactor.

With high-risk transaction approval functionality, banks can expect almost one out of every three people who bank online to adopt PhoneFactor.

Consumers Will Pay \$3.95 per Month To Banks

The Van Westendorp price modeling (Dutch economist Peter Van Westendorp) was employed in the survey to determine the optimal price point from the suppliers (Banks) perspective. In other words, the maximum price a consumer is willing to pay that also maximizes market share.

Four questions are used in the Van Westendorp design:

1. If this service were offered from your banking institution, at what price (on a monthly basis) would this service start to seem so CHEAP, you might not trust its quality?
(Enter a \$/month) ____/month
2. At what price (on a monthly basis) would this service start to seem like a BARGAIN to you?
(Enter a \$/month) ____/month
3. At what price (on a monthly basis) would this service start to seem EXPENSIVE to you?
(Enter a \$/month) ____/month
4. At what price (on a monthly basis) would this service be TOO EXPENSIVE for you to consider purchasing?
(Enter a \$/month) ____/month

The mean of the question #2 is considered to be the safe price-point and the mean of question #3 is considered to be the more aggressive price-point. \$3.80 per month (mean for question #2) is the point where consumers say PhoneFactor starts to seem like a bargain.

\$10.70 per month (mean for question #3) is the point where consumers say PhoneFactor starts to seem too expensive.

This is an unusually wide gap allowing advantageous pricing opportunity for banks (i.e. the price point is relatively inelastic between #2 and #3). But historically, psychological price points occur in context of the five dollar point.

It's suggested that the mean of the second bound question be used as an anchor price-point (\$3.80), with recommendation that the end consumer price-point be \$3.95 per month.

PhoneFactor a Cause to Switch Banks

Results indicate that PhoneFactor would be driver to switch banks for up to 34% of respondents with 4% being "extremely" or "very" likely to switch banks if the PhoneFactor service was offered from another bank for \$3.95 per month.

PhoneFactor – a Product For the Masses

Perhaps most surprising is the effect of income status on likelihood to adopt.

When adding on services of nominal fees (consider Call-Waiting with telephones), one expects to see the uptake in adoption higher with higher income brackets.

PhoneFactor does not follow this pattern.

Recall our normal "general interest" question before pricing is revealed six questions later in the survey instrument—it averaged 48% interest level for "extremely" and "very" interested.

As a frame of reference to the below data, as of August, 2007, the median U.S. Household Income was \$48,200.

Percentage “Extremely” and “Very” interested in PhoneFactor

48% = Mean

< \$50k HH Inc	\$50-\$99.9k HH Inc	\$100-\$149.9k HH Inc	\$150k+ HH Inc
55%	50%	42%	39%

Index to Avg “Extremely” and “Very” interested in PhoneFactor at \$3.95/month

100 = Mean

< \$50k HH Inc	\$50-\$99.9k HH Inc	\$100-\$149.9k HH Inc	\$150k+ HH Inc
105	120	90	75

PhoneFactor is not an elite-class product; the data show it’s a product for the masses.

Demographics of Respondents

In addition to full tables, summary demographics of the survey instrument respondents are outlined forthwith:

48% Male

52% Female

78% College Educated (57% undergrad, 21% graduate)

22% High School Educated

68% Employed Full-Time

11% Employed Part-Time

5% Self-Employed

4% Unemployed

75% White

10% Hispanic

9% African American/Black

2% Asian

40% <\$50k HH Inc

44% \$50k-\$99.999 HH Inc

11% \$100k-\$149.999 HH Inc

7% \$150k+ HH Inc

52% Married

30% Single Never Married

9% Divorced

7% Single Living with Partner

2% Widowed

1% Separated

Survey Methodology

The PhoneFactor survey was conducted online within the United States by Harris Interactive on behalf of Buzz Marketing & PR, Inc. between March 14 and March 20, 2008 among 1500 adults age 18+ who currently engage in online banking, online stock trading, or have checked credit card balances online. Results were weighted as needed for age, sex, race/ethnicity, education, region and household income.

All sample surveys and polls, whether or not they use probability sampling, are subject to multiple sources of error which are most often not possible to quantify or estimate, including sampling error, coverage error, error associated with nonresponse, error associated with question wording and response options, and post-survey weighting and adjustments. Therefore, Harris Interactive avoids the words “margin of error” as they are misleading. All that can be calculated are different possible sampling errors with different probabilities for pure, unweighted, random samples with 100% response rates. These are only theoretical because no published polls come close to this ideal.

Respondents for this survey were selected from among those who have agreed to participate in Harris Interactive surveys. The data have been weighted to reflect the composition of the online U.S. adult population. Because the sample is based on those who agreed to be invited to participate in the Harris Interactive online research panel, no estimates of theoretical sampling error can be calculated.

Harris Interactive was responsible for the data collection, while PhoneFactor’s agency was responsible for data analysis and reporting of results.