

To Avoid Phishing by Using Strong Authentication



To AVOID PHISHING BY USING STRONG AUTHENTICATION

Phishing

(FISH.ing) pp. Creating a replica of an existing Web page to fool a User into submitting personal, financial, or password data.

—adj. —phisher n.

Phishing is the term coined by hackers who imitate legitimate companies in e-mails to entice people to share passwords or credit-card numbers.

The term Phishing comes from the fact that Internet scammers are using increasingly sophisticated lures as they “fish” for Users’ financial information and password data.

Recurring patterns

The Fraudster targets Static Passwords.

Static Passwords are widely used for all kinds of purposes.

Static Passwords can be easily re-used by Fraudster.

Typical Phishing scheme:

Email is broadcast from a fake server address, pretending to be the real company or Financial Institution, containing an invitation to verify or to enter Username password

The fake website looks like the real one form the Financial Institution.

A Microsoft Internet Explorer programming code bug is used to display the address of the real website, masking the fake website address.

This is based upon some characters in the ‘url’, which are masking the real address of the website

Phishing Fraud Scheme

The goal is to obtain the Users’ static password by sending out massive amount of emails.

On the fake, but very real looking and feeling website, the Username/Password pair is collected.

In most cases, the gathered pairs of Username/Password can be processed in batch by the Fraudster any time afterwards. This is a batch process, which makes it more manageable, as the Fraudster has not to wait for Username/Password pairs to arrive.

VASCO’s strong authentication solution against Phishing: the Digipass product line

A Digipass is a token solution.

Digipass generates One Time Passwords upon request of the owner of the token, by entering PIN code on the token or pressing a button on the token.

Digipass contains internal real-time clock, which allows for Time-Based Passwords.

VASCO’s solution includes Server verification integration software, which is a C-Library with C-API for easy integration into any platform, on any operating system in any (legacy) software.

It is virtually impossible to misuse VASCO’s solution:

The generated Passwords are not only for One-Time use only, but also Time-Based Passwords. Replaying of passwords is controlled by server verification software.

Being Time-Based, forces the Fraudster to operate in (almost) real time.

Fraudster must sit in between Customer and financial institution for communication reasons between both parties.

Verification of passwords in real time:

This reduces the time for the Fraudster to act, due to expiration of the Password.

One Time Passwords:

Steal once, use one time only (and fast)

Batch processing of Username/Passwords is no longer possible for Fraudster.

This puts a time pressure on Fraudster.

Moreover instead of waiting for many passwords to be collected, the Fraudster now has to be present at the moment the Username/Password is revealed, as he has to use this pair immediately.

Security Layers

Where are the One Time Passwords situated in the layers:

Authentication	Static Password, Digipass, Certificates
Application security Layer	DES, 3-DES, AES, ...
Protocol Layer	SSL, Tunnels, ...
Access Security Layer	Firewalls, Routers, ...
Networking Security Layer	VPN, Leased Lines, ...
Physical Security	Building, Fiber protection, ...

Digipass Tokens – how do they work?

Every User has a personalized token.

Upon request the User can generate a Time Based One Time Password.

The User enters the One Time Password into the Password field, next to the Username field, as requested by the Server.

Just like he always has done with Username/Password.

The software on the Server uses the Username to get data from the Customer Data Base and the real time clock of the System to recalculate the One Time Password for this User.

The software verifies both Passwords to authenticate the User.

Token types:

1) With PIN:

Having a numeric keypad.

Note: The PIN has to be sent by mailer in order to let the User use the Digipass.

Another possibility is that the user needs to put in a PIN during first time usage.

Of course the PIN may be changed by User or can be forced to change during first time use.

2) Without PIN:

Easier to use and deploy

No PIN mailer to be sent (see argument above)

Less functionalities than with PIN, because no numeric keypad



Digipass tokens have several function possibilities:

1) Time-Based One Time Passwords

2) Time-Based Challenge/Response

3) Time-Based Signature function

4) Time-Based Host authentication

1) Time Based One Time Passwords

One time use only

One Time Passwords are time based

Typically 36 seconds before the next one is generated

The Server has a wider window than 36 seconds to accept the Password

The combination of unknown secrets, verification procedure and real time clock puts the Fraudster under time pressure. A wider time-window is decreasing the security. The length of the password is increasing the security.



2) Time Based Challenge/Response

First we have to explain the procedure of Challenge/Response:

- Users signs on with User ID
- Server/System to present Challenge to User
- User enters the Challenge into Digipass
- Digipass generates the Response
- User enters Response into System
- User gets authenticated by the System

This is a very complex process for Fraudster:
The Fraudster has to use Username immediately to get the appropriate current Challenge from the Server. So he needs to be connected already to the Server/Website.

Once he receives the Challenge, he needs to present the Challenge to the Customer.

The Customer can then generate a Response to Challenge using his Digi-pass

After receiving Response from the Customer, the Fraudster could try to make his fraudulent move, as the Response is again time based.

Not only the Fraudster has now to wait for a User to send Username, but the Fraudster now also needs to interact in the communication between User and Financial Institution passing the Challenge and getting the Response.



3) Signature function



A Financial Institution can request a Signature from the Customer for each transaction or important transaction.

This Signature contains encrypted data from the transaction:

Which can be Account number, Receiving Account Number, Amount, Date.

Moreover this Signature is again Time Based.

The transaction data cannot be altered, as the Signature needs to change too. In this case there is no opportunity for Fraudster at all.

4) Host/website authentication

This solution allows the User to authenticate his Bank, in order to verify the authenticity of the website.

How:

A function on the DigiPass allows for this.

Internally the DigiPass generates a long Time Based One Time Password.

Only first part is shown to User on the display of the DigiPass.

The User enters this part into the website of the Bank.

Bank receives Username & first part Password.

The system of the Bank calculates latter part of the Password and sends it to User.

The User enters latter part of the Password into his DigiPass for verification.

If correct the DigiPass will let know the User.



DigiPass & EMV authentication for Credit- and Debit Cards:

EMV stands for Europay MasterCard VISA

EMV is a Payment Application on Smart Card for Credit- & Debit Cards.

A WorldWide standard for all MasterCards (=Europay) and VISA cards.

Although originally meant for more security during physical Payments, it can also be used in the "Virtual World" too. The Card Not Present payments.

For this authentication, the User uses the same PIN as when paying in a local shop or grocery store. Thus the same PIN as for the ATM machine.



In order to authenticate himself, the customer uses:

- an UnConnected Smart Card Reader
- or
- an USB Connected Smart Card Reader

“One Chip One PIN for Everything”

With the Smart Card (Chip) on his Credit- or Debit Card and the Only PIN the user ever uses with this card, he is able to authenticate himself for Every channel from his Bank:

- e-Commerce, (Mail Order)/Telephone Order and Internet transactions
- Internet- & Telephone Banking

This makes his life as a Customer much more easy and more convenient.

There also many benefits for the Bank involved in less Operating-, Marketing- and Support costs. Moreover it brings branding in the hands of the User.

Thus Everything from ATM, POS to e-Commerce and Remote Banking is accessible with the One same Chip and One same PIN for the Customer.

The Authentication Integration:

1) e-Banking and Telephone Banking:

No separate authentication server required

Our solution can be installed on Operating System into any (legacy) software.

The product VASCO uses is Vacman Controller:

This is a C-Library with C-API, which allows for easy and fast integration

Using the existing Application Client Data Base

The Vacman Controller is in use with over 250 Financial Institutions.

2) E-Commerce integration

VASCO's authentication solution has already been integrated into 3D-Secure schemes:

- SecureCode from MasterCard
- Verified By VISA from VISA

By several Market leading Vendors (amongst others):

- CYOTA
- Element
- ARCOT

3) Remote Access & Corporate Network Access

The authentication solution from VASCO has been integrated in Firewalls, VPN, Radius servers, Portal softwares, ... from many Vendors:

Netscreen, Lucent Technologies, Stonesoft, Funk Software, CheckPoint, Integric, CISCO, Columbitech, Netilla, Avaya, Evidian, Citrix, Microsoft, NetworkEngines, Novell, Netegrity, Nomadix, Whale Communications, PassGo, Protocom, Sonicwall, Uroam, ...

DIGIPASS FACTORY
A concept for Strong User Authentication & Digital Signatures

FROM:
- Transactions with high value
- High frequency of use

TO:
- Transactions with low value
- Low frequency of use

ONE IN RESTRUCTURE FOR ALL DIGIPASS

DIGIPASS FACTORY
THE AUTHENTICATION COMPANY

VASCO

Pro 550, Pro 560, Go 1, Desk 850, Pro 200, Pro 210, Pro 220, Go 2, for Palm, for S/M, for Windows, Digipass Authentication server, Pro 800, Pro 300, Go 1, for Palm OS, Pro 200, Pro 210, Pro 220, Go 2, for Palm, for S/M, for Windows, Digipass Authentication server

Americas

VASCO Data Security Inc.
1901 South Meyers Road, Suite 210
Oakbrook Terrace, Illinois 60181, USA
Tel: +1 630 932 8844
Fax: +1 630 932 8852
E-mail: info_usa@vasco.com

EMEA

VASCO Data Security nv/sa
Koningin Astridlaan 164
B-1780 Wemmel, Brussel
Tel: +32 2 456 98 10
Fax: +32 2 456 98 20
E-mail: info_europe@vasco.com

APAC

VASCO Data Security Asia-Pacific Pte Ltd.
14-00 Prudential Tower, 30 Cecil street
049712 Singapore
Tel: +65 6 232 2727
Fax: +65 6 232 2888
E-mail: info_asia@vasco.com