

1. Le message, son aspect général :

Les clients VISA sont la cible par une tentative de phishing.

L'objet du message est :

Attention! Several VISA Credit Card bases have been LOST!

----- Message original -----

Sujet:Attention! Several VISA Credit Card bases have been LOST!

Date:Fri, 3 Feb 2006 09:38:46 -0100

De:VISA Service <VisaCard@visa.com>

Pour:

Good afternoon, unfortunately some processings have been cracked by hackers, so a new secure code to protect your data has been introduced by visa.

You should check your card balance and in case of suspicious transactions immediately contact your card issuing bank.

If all transactions are alright, it doesn't mean the card is not lost and cannot be used. Probably, your card issuers have not updated information yet.

That is why we strongly recommend you to visit our web-site and update your profile, otherwise we cannot guarantee stolen money repayment.

Thank you for your attention.

Click [here](#) and update your profile.

2. La technique utilisée :

La technique est celle du classique lien à cliquer « Click [here](#) ».

Le code html montre l'adresse du site hébergeant le phishing :

Click here and update your profile.

Lors de nos essais, nous avons constaté que les images sont téléchargées à partir du site :

72.36.222.12.reversedns.resolve.ru

L'ensemble est très « sobre » et certainement très « efficace » ceci malgré l'usage de la langue anglaise.

La page associée au lien indiqué est la suivante :

Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Mail Print

Address <http://72.36.222.12/lostvisa/index.php> Go

VISA VISA EUROPE

I want Visa **I've lost my Visa** **Accepting Visa** **I use Visa** **My Future Visa** **Downloads**

Lost cards
Travellers cheques
Keep your card safe

Attention

Because of frequent hacker and charlatan attacks several visa bases have been stolen. Your card might be in the lost base and have already fallen among thieves. You should check your card balance and in case of suspicious transactions immediately contact your card issuing bank.

If all transactions are alright, it doesn't mean the card is not lost and cannot be used. Probably, your card issuers have not updated information yet. You will fill, if you please, form for obtaining Visa secure code, this code will allow you to preserve their economy in the soundness and safety, and it will be known only to you. You will preserve attention, and you will better memorize this code and give no one.

Attention! After the incidents banks must block all online access to cards.

If you have online access to your credit card or online access to the bank - your card issuing bank, fill in the bands. We will send your data to your card issuing bank for your accounts not to be blocked.

Assistance

Attention!

After the incidents banks must block all online access to cards.

If you have online access to your credit card or online access to the bank - your card issuing bank, fill in the bands. We will send your data to your card issuing bank for your accounts not to be blocked. 24 hrs a day. 365 days a year.

Lost Cards:

Lost Travellers Chqs:

VISA SECURE **SSL 128BIT**

Credit Card Number*:

Credit Card Expire Date*:
 example - mm / yy /

Last 3 digits on Signature Panel*:

PIN Code*:
 4 Digit code used in ATM machines

Social Security Number*:
 Do not use special characters (= < > ") .

Security Word or Mother's Maiden Name*:

Security word you provided when you applied for your card or your mother's maiden name--last name only. Do not use special characters (= < > ") .

Your Birth Day*:
 example - dd / mm / yy / /

Your Full Name*:
 exactly printed on card .

Country*:

Your Address*:
 associated with your card.

Your City*:
 associated with your card.

Your Address's Zipcode*:

Preparing for international travel?

Let Visa help.

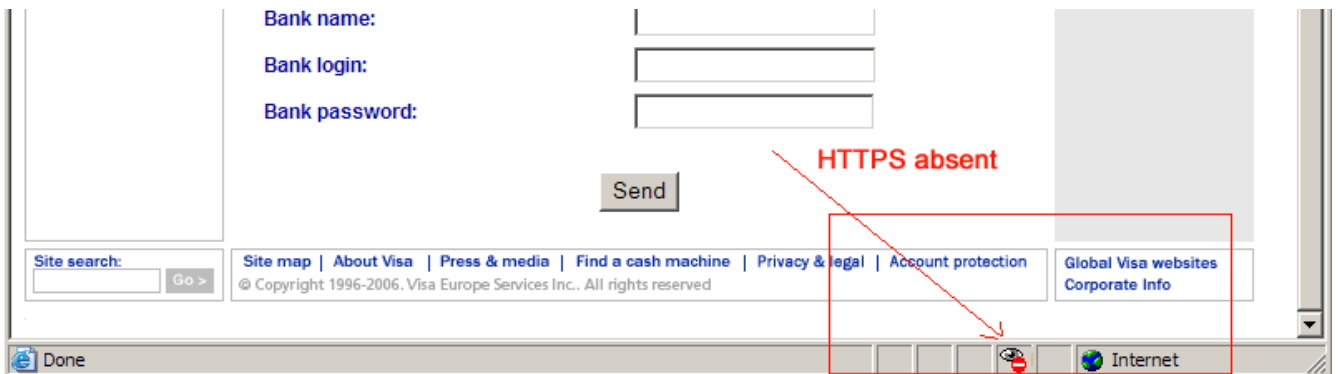
Download this free application onto your Palm handheld and have both Visa toll-free global assistance nos. and international travel tips on hand at all times.

Palm OS v3.1 or higher recommended.

Visa Lost Card v1.0
[Download: zip \(70k\)](#)
[Download: sit \(70k\)](#)

Done Internet

L'absence de session sécurisée via HTTPS et la présence d'un formulaire d'accès avec des informations confidentielles sur la page d'accueil sont caractéristiques du phishing :



Si des informations (aléatoires !) sont fournies, le résultat est classique. Il consiste à rediriger vers une page d'erreur pour essayer de leurrer l'internaute :

Visa | I've lost my Visa - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Mail Print

Address <http://72.36.222.12/lostvisa/index.php?error=er42> Go

VISA VISA EUROPE

I want Visa **I've lost my Visa** Accepting Visa I use Visa My Future Visa Downloads

Lost cards
Travellers cheques
Keep your card safe

Attention

Because of frequent hacker and charlatan attacks several visa bases have been stolen. Your card might be in the lost base and have already fallen among thieves. You should check your card balance and in case of suspicious transactions immediately contact your card issuing bank.

If all transactions are alright, it doesn't mean the card is not lost and cannot be used. Probably, your card issuers have not updated information yet. You will fill, if you please, form for obtaining Visa secure code, this code will allow you to preserve their economy in the soundness and safety, and it will be known only to you. You will preserve attention, and you will better memorize this code and give no one.

Attention! After the incidents banks must block all online access to cards.

If you have online access to your credit card or online access to the bank - your card issuing bank, fill in the bands. We will send your data to your card issuing bank for your accounts not to be blocked.

Assistance

Attention!
After the incidents banks must block all online access to cards.

If you have online access to your credit card or online access to the bank - your card issuing bank, fill in the bands. We will send your data to your card issuing bank for your accounts not to be blocked. 24 hrs a day. 365 days a year.

Lost Cards:
Select Country

Lost Travellers Chqs:
Select Country

VISA SECURE SSL 128BIT

Preparing for international travel?
Let Visa help.
Download this free application onto your Palm handheld and have both Visa toll-free global assistance nos. and international travel tips on hand at all times.
Palm OS v3.1 or higher recommended.
Visa Lost Card v1.0
Download: zip (70k)
Download: sit (70k)

Credit Card Number*: 714457891455568

Credit Card Expire Date*: example - mm / yy 06 / 06

Last 3 digits on Signature Panel*: 779

PIN Code*: 4 Digit code used in ATM machines ●●●●

Social Security Number*: Do not use special characters (= < > ") . 1221221224

Security Word or Mother's Maiden Name*: anne

Security word you provided when you applied for your card or your mother's maiden name--last name only. Do not use special characters (= < > ") .

Your Birth Day*: example - dd / mm / yy

Your Full Name*: _____

3. Identification de l'origine du phishing

L'outil Whois permet de remonter la trace jusqu'à la Fédération de Russie :

```
Layered Technologies, Inc. LAYERED-TECH- (NET-72-36-128-0-1)
    72.36.128.0 - 72.36.255.255
Internet Technologies Ltd INTERNET-TECHNOLOGIES-LTD (NET-72-36-244-129-1)
    72.36.244.129 - 72.36.244.255
```

```
72.36.222.12.reversedns.resolve.ru
```

```
domain:  RESOLVE.RU
type:    CORPORATE
descr:   Internet Technologies Ltd.
nserver: rslv5.resolve.ru. 72.36.244.253
nserver: rslv6.resolve.ru. 72.36.245.41
state:   REGISTERED, DELEGATED
person:  Dmitriy G Danilev
```

phone: +7 905 2006861

+7 est l'indicatif international de la Fédération de Russie !!!

```
fax-no:  +7 812 7406861
e-mail:  dmitry@resolve.ru
e-mail:  abuse@resolve.ru
e-mail:  ipnet@resolve.ru
registrar: REGTIME-REG-RIPN
created: 2004.10.04
paid-till: 2006.10.04
source:  TC-RIPN
```

```
MX-record for resolve.ru.:
```

```
Preference = 0
Mail server = resolve.ru.
TTL = 4 Hours
```

```
SOA-record for resolve.ru.:
```

```
Primary DNS server = rslv5.resolve.ru.
Responsible person = sales.resolve.ru.
Serial number = 2005102704
Refresh interval = 1 Day
Retry interval = 2 Hours
Expire interval = 41 Days, 16 Hours
Default / minimum TTL = 1 Day
TTL = 1 Day
```

```
NS-record for resolve.ru.:
```

```
DNS server = rslv5.resolve.ru.
TTL = 1 Day
```

```
NS-record for resolve.ru.:
```

```
DNS server = rslv6.resolve.ru.
TTL = 1 Day
```

```
A-record for resolve.ru.:
```

```
IP address = 72 36 244 250
```

4. Actions engagées

- La publication de ce document,
- Information faite à l'organisation VISA,
- Ce cas a été reporté au niveau « .org »,