The Invisible Threat – MitB (Man in the Browser)

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- Uri Fleyder
- Security Researcher
- FraudAction Research Lab @ RSA

OWASP
The Open Web Application Security Project

- Plan for the following 28 minutes:
  - Get familiar with the MitB threat
  - Live demonstration
  - Discuss possible solutions

- Video demonstration

..\Video\MitB.mxf

OWASP
The Open Web Application Security Project

- Do you trust your endpoint device?

- Desktop PC
- Laptop
- Notebook
- Mobile phone

OWASP
The Open Web Application Security Project

- What is trust?

- Definition for trust @ thefreedictionary.com:

"The condition and resulting obligation of having confidence placed in one"

OWASP
The Open Web Application Security Project

- Your endpoint device can be compromised in numerous ways by various techniques, with or without the user's active intervention

OWASP
The Open Web Application Security Project

- Malicious links via spam emails and messages in social networks
- Malicious executable files via file sharing services and free download websites
- Drive-by exploits
- Built-in backdoors in legitimate software
- Malicious worms - spreading inside and outside your LAN

- Most of the users trust their endpoint device
- They will follow almost any instructions displayed by the web-browser
- The instructions should be written, displayed or shown in a reliable enough manner (correct context, spelling, grammar).

OWASP
The Open Web Application Security Project

- Let us assume that you are using your own PC in order to log in to your online banking account and displayed with one of the following:

OWASP

The Open Web Application Security Project

Validate Security Information

Your security is important to us, so please answer your security question before logging in.

SUBMIT REQUEST | RESET | CANCEL

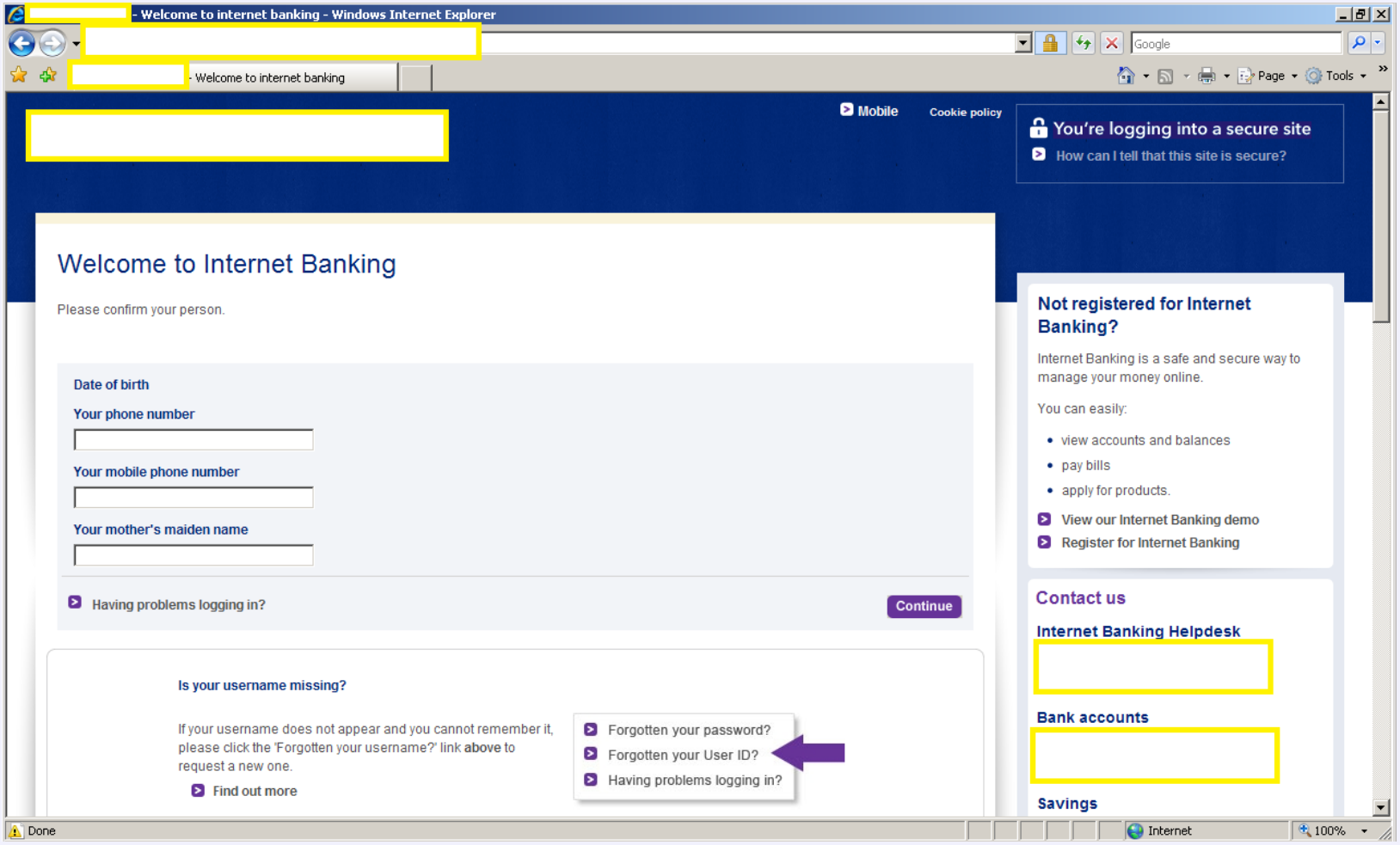
Enter your User ID and Password below:

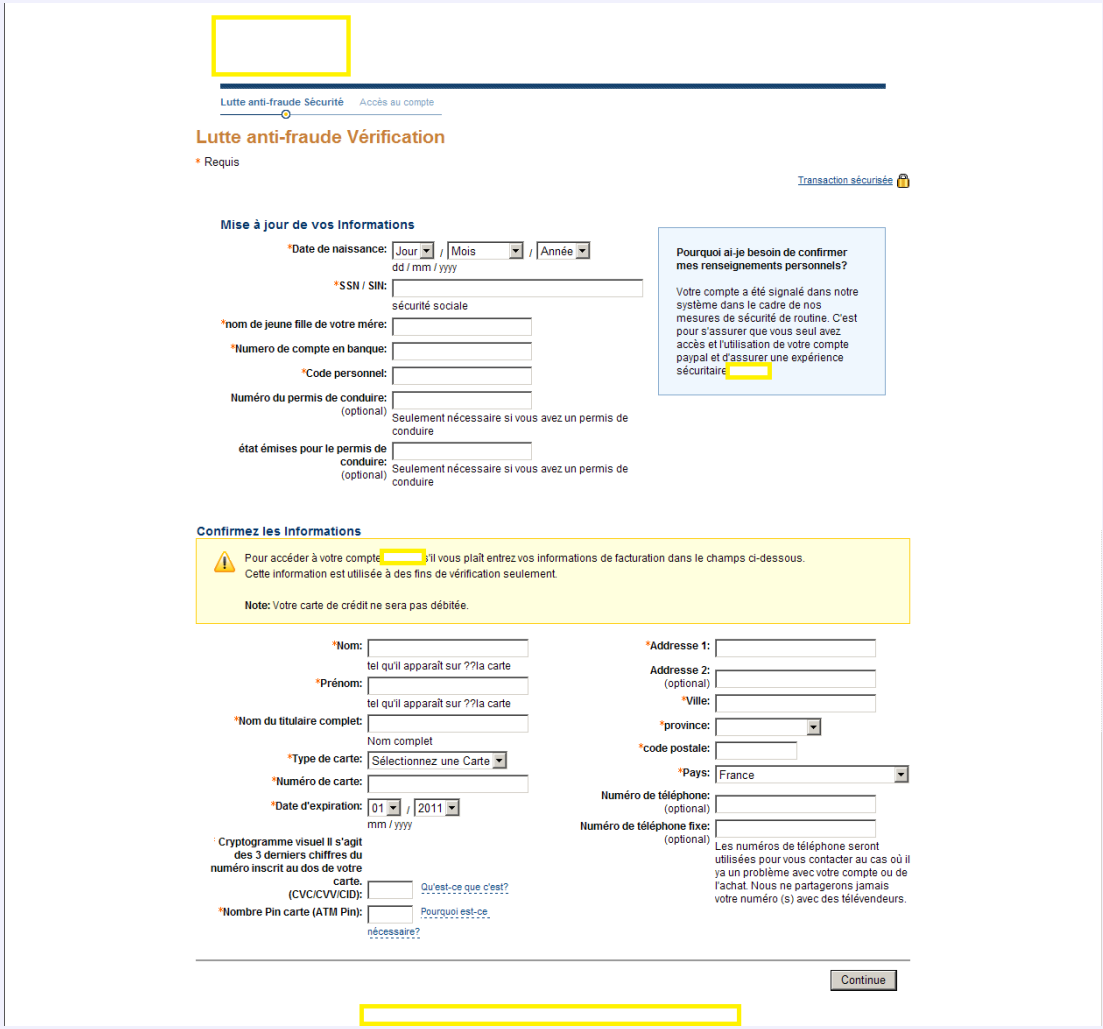
User ID:

Password:

LOG IN

Have you forgotten your User ID or Password?


- Welcome to internet banking - Windows Internet Explorer
Google
- Welcome to internet banking
Page
Tools
Mobile
Cookie policy
You're logging into a secure site
How can I tell that this site is secure?
Welcome to Internet Banking
Please confirm your person.
Date of birth
Your phone number
Your mobile phone number
Your mother's maiden name
Having problems logging in?
Continue
Is your username missing?
If your username does not appear and you cannot remember it, please click the 'Forgotten your username?' link above to request a new one.
Find out more
Forgotten your password?
Forgotten your User ID?
Having problems logging in?
Not registered for Internet Banking?
Internet Banking is a safe and secure way to manage your money online.
You can easily:
view accounts and balances
pay bills
apply for products.
View our Internet Banking demo
Register for Internet Banking
Contact us
Internet Banking Helpdesk
Bank accounts
Savings
Done
Internet
100%



Lutte anti-fraude Sécurité — Accès au compte

Lutte anti-fraude Vérification

* Requis

Transaction sécurisée

Mise à jour de vos Informations

*Date de naissance: Jour / Mois / Année
dd / mm / yyyy

*SSN / SIN:
sécurité sociale

*nom de jeune fille de votre mére:

*Numero de compte en banque:

*Code personnel:

Numéro du permis de conduire: (optional)
Seulement nécessaire si vous avez un permis de conduire

état émises pour le permis de conduire: (optional)
Seulement nécessaire si vous avez un permis de conduire

Pourquoi ai-je besoin de confirmer mes renseignements personnels?

Votre compte a été signalé dans notre système dans le cadre de nos mesures de sécurité de routine. C'est pour s'assurer que vous seul avez accès et l'utilisation de votre compte paypal et d'assurer une expérience sécuritaire

Confirmez les Informations

Pour accéder à votre compte, s'il vous plaît entrez vos informations de facturation dans le champs ci-dessous.
Cette information est utilisée à des fins de vérification seulement.

Note: Votre carte de crédit ne sera pas débitée.

*Nom:
tel qu'il apparaît sur ??la carte

*Prénom:
tel qu'il apparaît sur ??la carte

*Nom du titulaire complet:
Nom complet

*Type de carte: Sélectionnez une Carte

*Numéro de carte:

*Date d'expiration: 01 / 2011
mm / yyyy

Cryptogramme visuel Il s'agit des 3 derniers chiffres du numéro inscrit au dos de votre carte. (CVC/CVV/CID): Qu'est-ce que c'est?

*Nombre Pin carte (ATM Pin): Pourquoi est-ce nécessaire?

*Addresse 1:

Addresse 2: (optional)

*Ville:

*province:

*code postale:

*Pays: France

Numéro de téléphone: (optional)

Numéro de téléphone fixe: (optional)

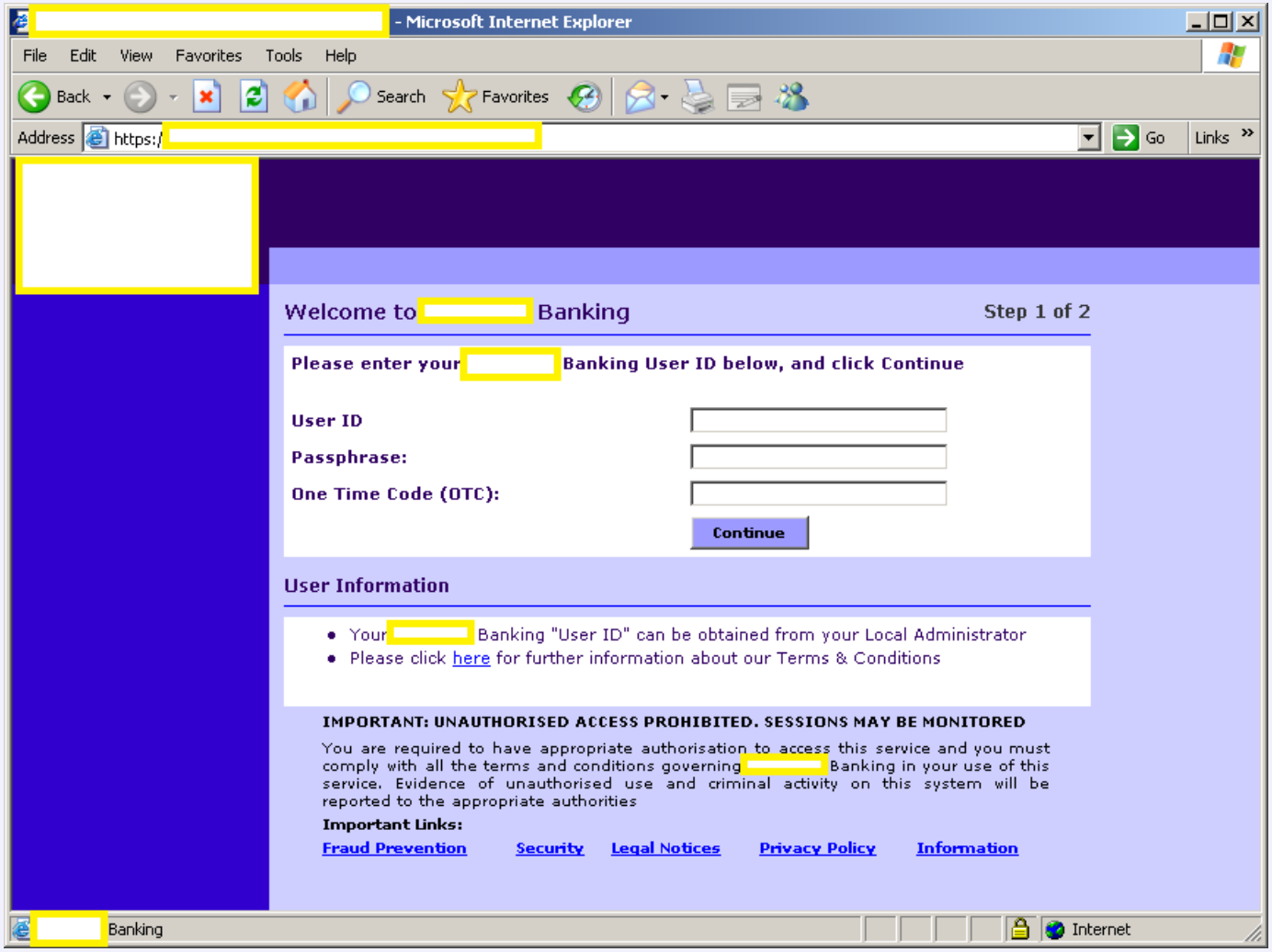
Les numéros de téléphone seront utilisées pour vous contacter au cas où il ya un problème avec votre compte ou de l'achat. Nous ne partagerons jamais votre numéro (s) avec des télévendeurs.

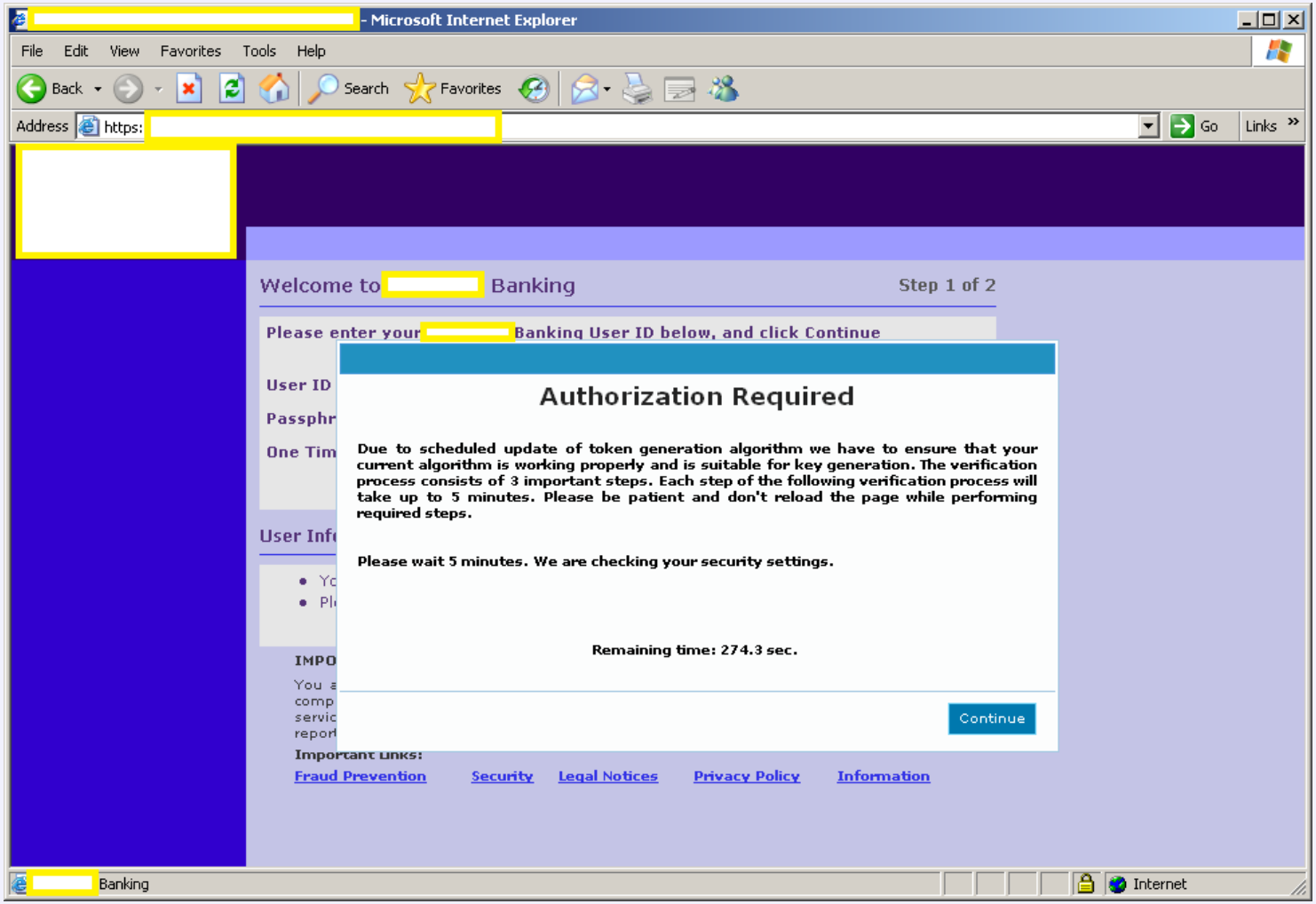
Continue

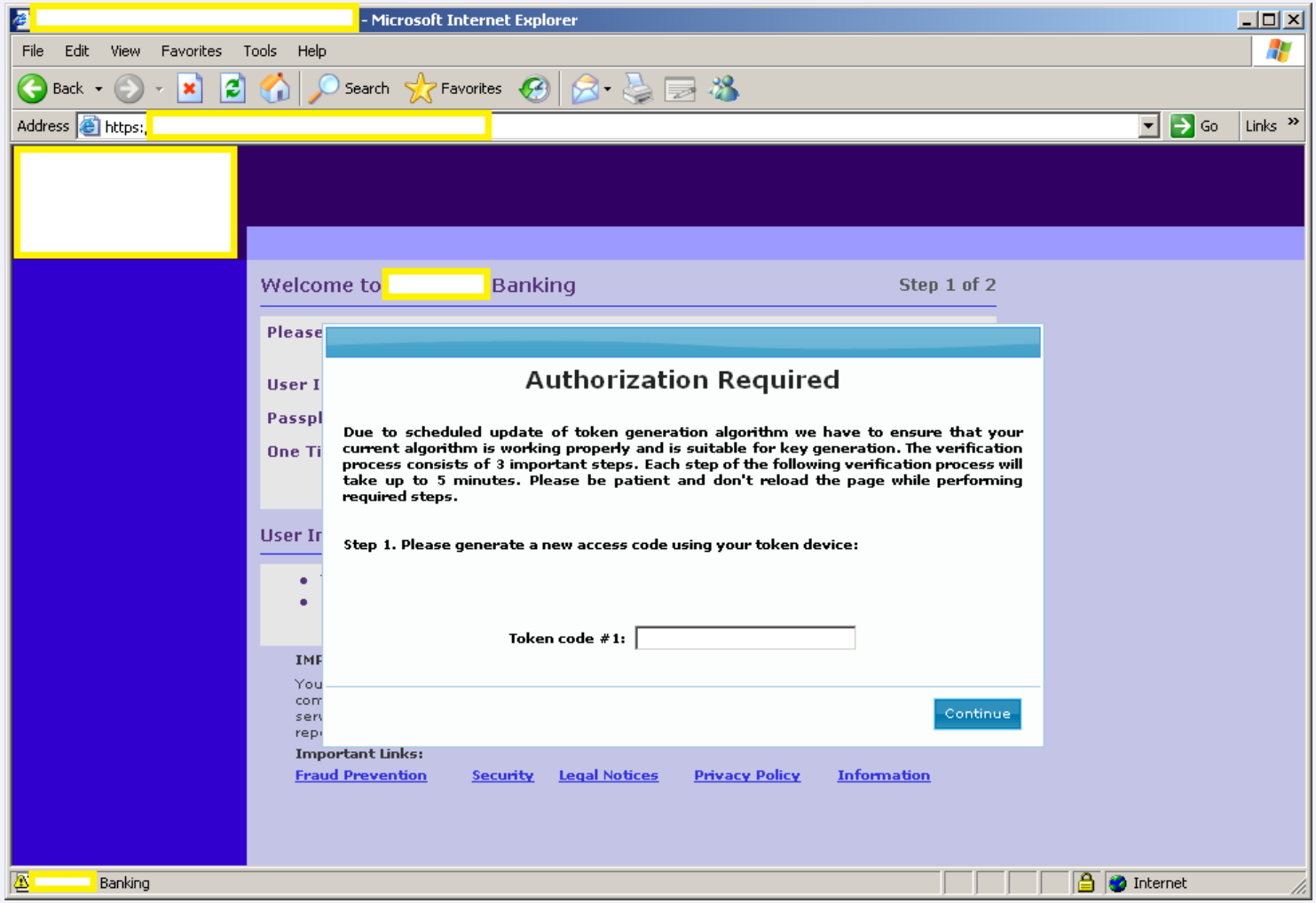
OWASP
The Open Web Application Security Project

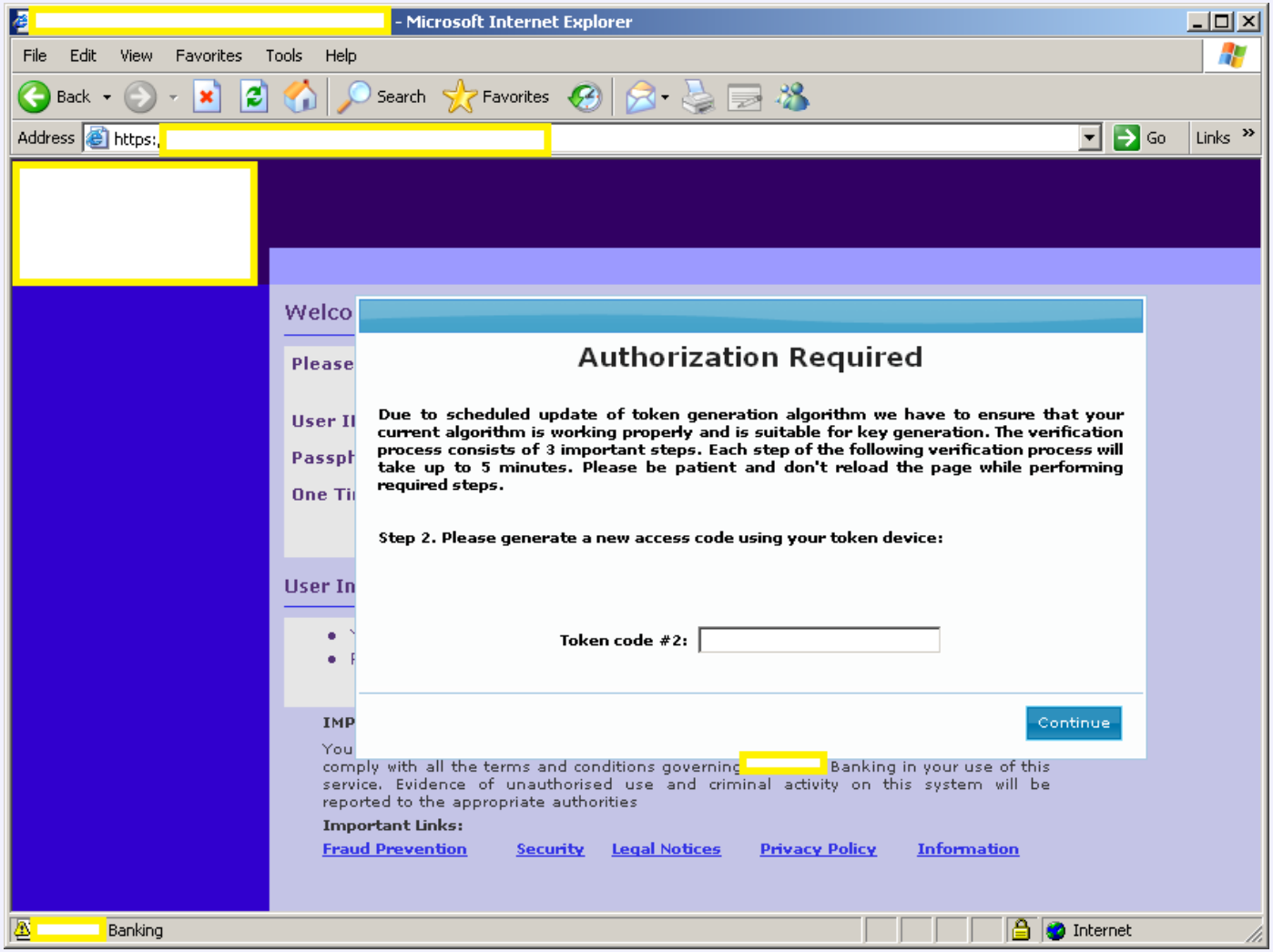
- How would you react?

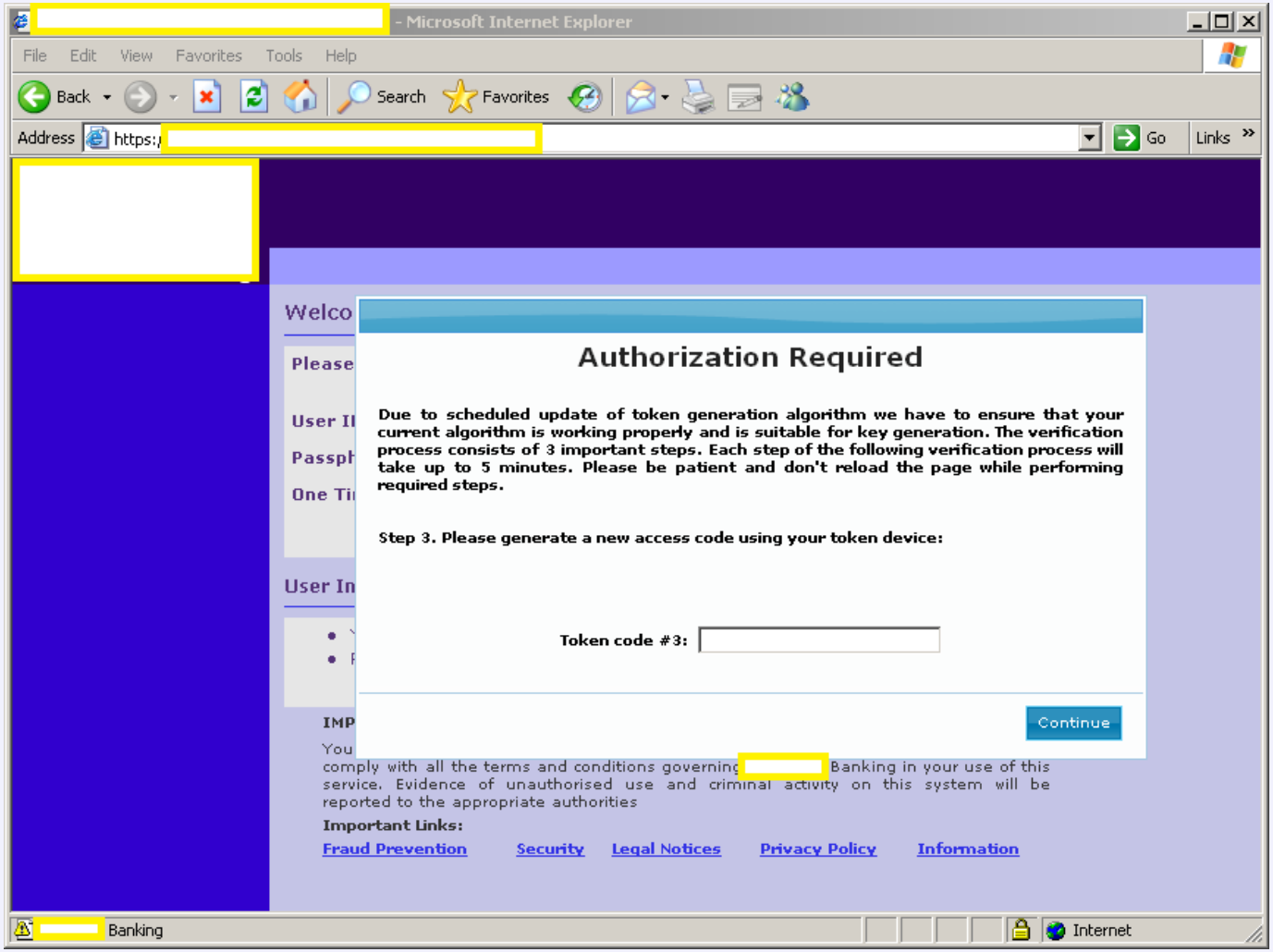
- Most of the users would not suspect that something is "phishy" here, many of them will follow the instructions and provide the requested information

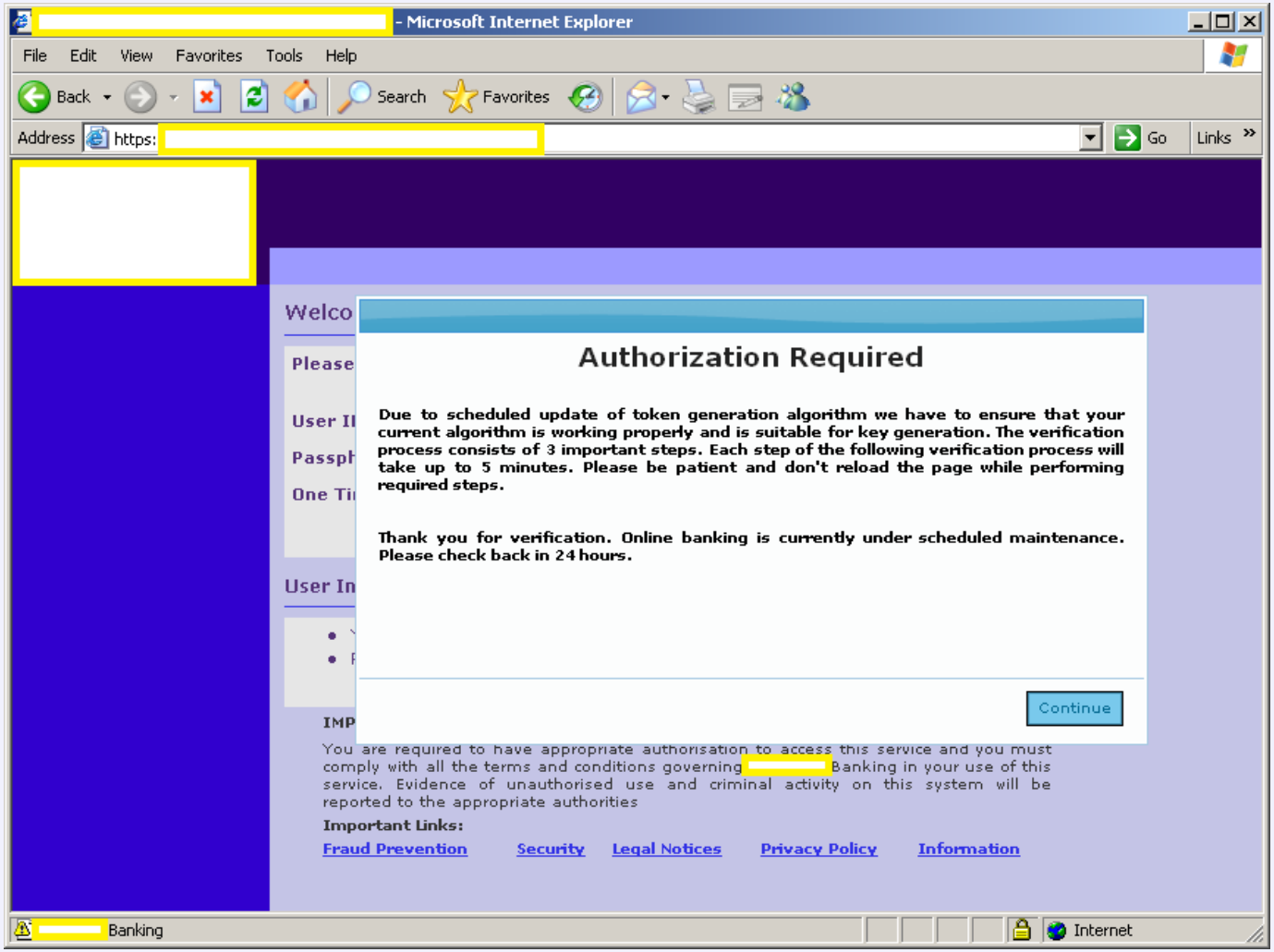

- Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https:/
Go Links
Welcome to Banking
Step 1 of 2
Please enter your Banking User ID below, and click Continue
User ID
Passphrase:
One Time Code (OTC):
Continue
User Information
Your Banking "User ID" can be obtained from your Local Administrator
Please click here for further information about our Terms & Conditions
IMPORTANT: UNAUTHORISED ACCESS PROHIBITED. SESSIONS MAY BE MONITORED
You are required to have appropriate authorisation to access this service and you must comply with all the terms and conditions governing Banking in your use of this service. Evidence of unauthorised use and criminal activity on this system will be reported to the appropriate authorities
Important Links:
Fraud Prevention
Security
Legal Notices
Privacy Policy
Information
Banking
Internet

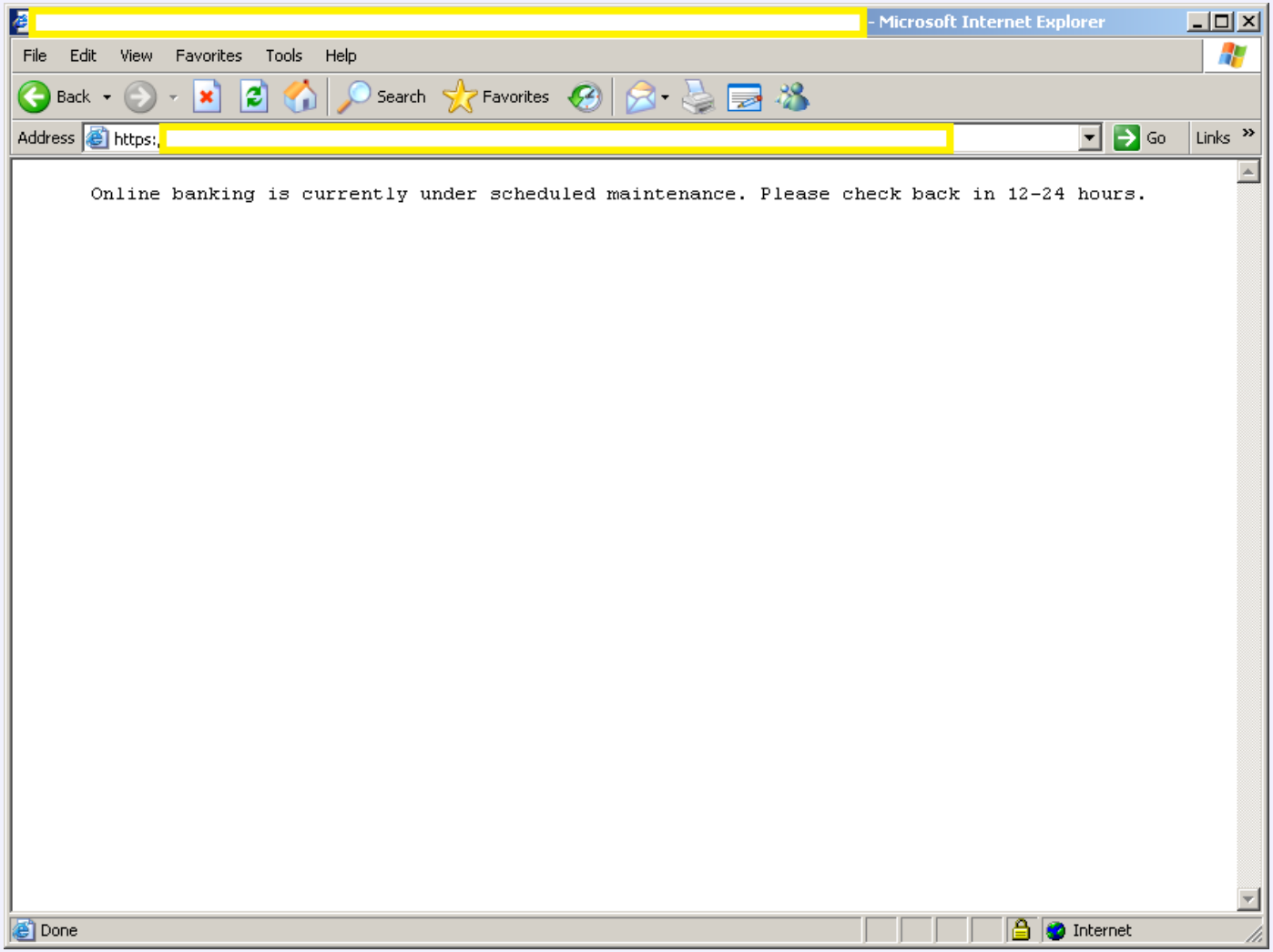

- Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https:
Go Links
Welcome to Banking
Step 1 of 2
Please enter your Banking User ID below, and click Continue
User ID
Passphr
One Tim
User Inf
Authorization Required
Due to scheduled update of token generation algorithm we have to ensure that your current algorithm is working properly and is suitable for key generation. The verification process consists of 3 important steps. Each step of the following verification process will take up to 5 minutes. Please be patient and don't reload the page while performing required steps.
Please wait 5 minutes. We are checking your security settings.
Remaining time: 274.3 sec.
Continue
Important Links:
Fraud Prevention
Security
Legal Notices
Privacy Policy
Information
Banking
Internet


- Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https:
Go Links
Welcome to Banking
Step 1 of 2
Authorization Required
Due to scheduled update of token generation algorithm we have to ensure that your current algorithm is working properly and is suitable for key generation. The verification process consists of 3 important steps. Each step of the following verification process will take up to 5 minutes. Please be patient and don't reload the page while performing required steps.
Step 1. Please generate a new access code using your token device:
Token code #1:
Continue
Important Links:
Fraud Prevention
Security
Legal Notices
Privacy Policy
Information
Banking
Internet


- Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https:
Go Links
Authorization Required
Due to scheduled update of token generation algorithm we have to ensure that your current algorithm is working properly and is suitable for key generation. The verification process consists of 3 important steps. Each step of the following verification process will take up to 5 minutes. Please be patient and don't reload the page while performing required steps.
Step 2. Please generate a new access code using your token device:
Token code #2:
Continue
comply with all the terms and conditions governing Banking in your use of this service. Evidence of unauthorised use and criminal activity on this system will be reported to the appropriate authorities
Important Links:
Fraud Prevention Security Legal Notices Privacy Policy Information
Banking
Internet


- Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https:
Go Links
Welco
Please
User I
Passph
One Ti
User In
Authorization Required
Due to scheduled update of token generation algorithm we have to ensure that your current algorithm is working properly and is suitable for key generation. The verification process consists of 3 important steps. Each step of the following verification process will take up to 5 minutes. Please be patient and don't reload the page while performing required steps.
Step 3. Please generate a new access code using your token device:
Token code #3:
Continue
IMP
You
comply with all the terms and conditions governing Banking in your use of this service. Evidence of unauthorised use and criminal activity on this system will be reported to the appropriate authorities
Important Links:
Fraud Prevention Security Legal Notices Privacy Policy Information
Banking
Internet


- Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https:
Go Links
Welco
Please
User I
Passph
One Ti
User In
Authorization Required
Due to scheduled update of token generation algorithm we have to ensure that your current algorithm is working properly and is suitable for key generation. The verification process consists of 3 important steps. Each step of the following verification process will take up to 5 minutes. Please be patient and don't reload the page while performing required steps.
Thank you for verification. Online banking is currently under scheduled maintenance. Please check back in 24 hours.
Continue
IMP
You are required to have appropriate authorisation to access this service and you must comply with all the terms and conditions governing Banking in your use of this service. Evidence of unauthorised use and criminal activity on this system will be reported to the appropriate authorities
Important Links:
Fraud Prevention
Security
Legal Notices
Privacy Policy
Information
Banking
Internet


- Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https:
Go Links
Online banking is currently under scheduled maintenance. Please check back in 12-24 hours.
Done
Internet

- People tend to trust their endpoint devices more than they trust 3-party service providers

- Typical user:

"this annoying bank is probably upgrading their website, oh well…"

OWASP
The Open Web Application Security Project

- The endpoint devices in all of the above cases were compromised by a financial Trojan with MitB capabilities
- MitB capable Trojans are using code hooks in order to inject predefined malicious content into the relevant process
  - iexplore.exe
  - firefox.exe
  - chrome.exe
  - opera.exe
  - explorer.exe

OWASP
The Open Web Application Security Project

- MitB?
  - No man (and no woman) inside
  - It is all about customized, tailor made (per target) client side code snippet (JavaScript), injected into the active process responsible for web browsing

OWASP
The Open Web Application Security Project

- Simple HTML injections
  - The web browser displays false information in order to steal additional personal and financial information
- ATS (Automatic Transfer System)
  - Malicious client side injections are capable to automatically transfer money from your banking account
- Manual MitB
  - Malicious client side injections are capable to send the login credentials to the fraudster in real time while blocking the user

OWASP
The Open Web Application Security Project

- During the last 3 years our research lab studied and analyzed more than 11,000 unique variants of financial Trojans

- All of the analyzed variants used client side injections

- Demonstration
  - Install of financial Trojan kit
  - Install of Exploit kit
  - Configuration of client side injections

- Solutions?
  - Web injections are triggered by visiting specific URL/domain - Changing the URL/domain is not feasible
  - Injected code usually relies on the DOM's objects, randomization and obfuscation of the DOM's namespace will disable most of the current MitB injections

- Questions?

- Please rate my talk ☺

https://www.surveymonkey.com/s/Research12_UriFleyder