AuntieTuna

Personalized Content-based Phishing Detection

Calvin Ardi, John Heidemann
Welcome to Internet Banking

If you don't already use Internet Banking, it's simple to register online.

Please enter your password and User ID (if you have forgotten your User ID simply click on the link 'Forgotten your User ID' and follow the instructions).

User ID: 
Password: 

[ ] Remember my User ID

Warning: Don't tick this box if you're using a public or shared computer

- Forgotten your password?
- Forgotten your User ID?
- Having problems logging in?

DOWNLOAD OUR FAST NEW MOBILE BANKING APP NOW

Save precious time in your day, with our secure three tap log on. Find out more.

Find out more

Helpful

Now you can get your Mortgage moving by booking an appointment online with your local advisor.

Book now

Contact Us....

Help & Support

Payments

Send money abroad, simply with Online International Payments.

Find out more

Protecting your money

find out more here
Welcome to Internet Banking

If you don’t already use Internet Banking, it’s simple to register online.

Please enter your password and User ID (if you have forgotten your User ID simply click on the link ‘Forgotten your User ID’ and follow the instructions).

User ID: [Please enter a value.]
Password: [Please enter a value.]
Remember my User ID: [Optional]

Warning: Don’t tick this box if you’re using a public or shared computer.

Forgotten your password? [Optional]
Forgotten your User ID? [Optional]
Having problems logging in? [Optional]

DOWNLOAD OUR FAST NEW MOBILE BANKING APP NOW
Save precious time in your day, with our secure three tap log on. Find out more.

iPhone and Android users only. Personal UK Internet Banking customers with an eligible account only. Device registration required. T&Cs apply.

HELPFUL
Now you can get your Mortgage moving by booking an appointment online with your local advisor.

YOUR HOME MAY BE REPOSSESSED IF YOU DO NOT KEEP UP REPAYMENTS ON YOUR MORTGAGE

Contact Us....

Help & Support

PAYMENTS
Send money abroad, simply with Online International Payments.

Find out more

Protecting your money find out more here
Welcome to Internet Banking

If you don’t already use Internet Banking, it’s simple to register online.

Please enter your password and User ID (if you have forgotten your User ID simply click on the link ‘Forgotten your User ID’ and follow the instructions).

- **User ID:**
  - Please enter a value.

- **Password:**

- [ ] Remember my User ID

**Warning:** Don’t tick this box if you’re using a public or shared computer.

- Forgotten your password?
- Forgotten your User ID?
- Having problems logging in?

DOWNLOAD OUR FAST NEW MOBILE BANKING APP NOW

Save precious time in your day, with our secure three tap log on. Find out more.

iPhone and Android users only. Personal UK Internet Banking customers with an eligible account only. Device registration required. T&Cs apply.

HELPFUL

Now you can get your Mortgage moving by booking an appointment online with your local advisor.

Book now

YOUR HOME MAY BE REPOSSESSED IF YOU DO NOT KEEP UP REPAYMENTS ON YOUR MORTGAGE.

CONTACT US

Help & Support

PAYMENTS

Send money abroad, simply with Online International Payments.

Find out more

Protecting your money
find out more here
missing lock
wrong URL
lost time and $$$
we need something effective and usable
url blacklists

effective?

usable?
url blacklists

effective?

usable?

slow updates
url blacklists

effective?  \(\text{🐌} \)  slow updates

usable?  \(\text{🚧} \)  when updated
url whitelists

effective? 🐌

usable? 🚧
url whitelists

effective?  yes

usable?
url whitelists

effective?
yes

usable?
too restrictive
what targets do we track?
what targets do we track?
how to deal with our targets?
what targets do we track?
how to deal with our targets?
how to make it usable?
AuntieTuna

user personalization

precise content matching

usable design
Auntie Tuna

user personalization

precise content matching

usable design
AuntieTuna

user personalization (discovery)
precise content matching
usable design
Welcome to Internet Banking

If you don't already use Internet Banking, it's simple to register online.

Please enter your password and User ID (If you have forgotten your User ID simply click on the link 'Forgotten your User ID' and follow the instructions).

User ID:

Password:

[ ] Remember my User ID

Warning: Don't tick this box if you're using a public or shared computer

Forgotten your password?
Forgotten your User ID?
Having problems logging in?

UPDATE BROWSER
To remain safer online and for a better online experience, check that you're using the latest browser. Find out more.
trust on first use
Log in to your PayPal account.

Email

Password

Log In

Forgot your email or password?

Sign Up

Contact Us  Privacy  Legal  Worldwide
manual add
$\Rightarrow$ defense++
Auntie Tuna

user personalization (discovery)

precise content matching (detection)

usable design
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
dolor sit amet, consectetur adipiscing elit.

```html
<script>
window.alert("hello world")
</script>
```
attack payload
common elements ⇒ phish
effective?
do we find the phish?
TABLE I. **Classification of phish in two days of PhishTank reports, based on detection against PayPal. Sensitivity = 58.8%, Specificity = 100%**.

<table>
<thead>
<tr>
<th>Description</th>
<th>Num. Pages</th>
<th>%</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Candidates</td>
<td>2374</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unavailable</td>
<td>486</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ripped</td>
<td>1888</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>1764</td>
<td></td>
<td>TN = 1764</td>
</tr>
<tr>
<td>PayPal (image-based, <em>removed</em>)</td>
<td>39</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PayPal</td>
<td>85</td>
<td>100.0</td>
<td>FP = 0</td>
</tr>
<tr>
<td>Successfully detected</td>
<td>50</td>
<td>58.8</td>
<td>TP = 50</td>
</tr>
<tr>
<td>Direct rips</td>
<td>35</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whitespace norm.</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JavaScript obfuscation</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom-styled with minor PayPal content</td>
<td>35</td>
<td>41.2</td>
<td>FN = 35</td>
</tr>
</tbody>
</table>
TABLE I. **Classification of phish in two days of PhishTank reports, based on detection against PayPal. Sensitivity = 58.8%, Specificity = 100%**.

<table>
<thead>
<tr>
<th>Description</th>
<th>Num. Pages</th>
<th>%</th>
<th>TN = 1764</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adverts</td>
<td>2374</td>
<td>100.0</td>
<td>FP = 0</td>
</tr>
<tr>
<td>Unavailable</td>
<td>436</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ripped</td>
<td>1888</td>
<td>58.8</td>
<td>TP = 50</td>
</tr>
<tr>
<td>Other</td>
<td>1764</td>
<td>41.2</td>
<td>FN = 35</td>
</tr>
<tr>
<td><strong>PayPal</strong> (image-based, <em>removed</em>)</td>
<td>39</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PayPal</strong></td>
<td>85</td>
<td>100.0</td>
<td></td>
</tr>
<tr>
<td>Successfully detected</td>
<td>50</td>
<td>58.8</td>
<td></td>
</tr>
<tr>
<td>Direct rips</td>
<td>35</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whitespace norm.</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JavaScript obfuscation</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom-styled with minor PayPal content</td>
<td>35</td>
<td>41.2</td>
<td></td>
</tr>
</tbody>
</table>
usable?
<table>
<thead>
<tr>
<th>Website</th>
<th>Page Render</th>
<th>AuntieTuna</th>
</tr>
</thead>
<tbody>
<tr>
<td>google.com</td>
<td>327 (15)</td>
<td>144 (6)</td>
</tr>
<tr>
<td>paypal.com</td>
<td>349 (5)</td>
<td>20 (2)</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>5316 (1632)</td>
<td>167 (6)</td>
</tr>
<tr>
<td>en.wikipedia.org</td>
<td>321 (7)</td>
<td>75 (3)</td>
</tr>
</tbody>
</table>
en.wikipedia.org
en.wikipedia.org

AuntieTuna
Auntie Tuna

user personalization (discovery)
precise content matching (detection)
usable design
one button

- add to good list
- messages
- all systems go.
100% automation
Warning—Suspected phishing page!

This page may be a forgery designed to trick you into sharing sensitive information. Entering any information here may result in identity theft or other abuse.

→ What is phishing and how do I protect myself? Click to learn more: antiphishing.org

→ We think you meant to go to: PayPal (paypal.com)

Back to Safety
Warning—Suspected phishing page!

This page may be a forgery designed to trick you into sharing sensitive information. Entering any information here may result in identity theft or other abuse.

→ What is phishing and how do I protect myself? Click to learn more: antiphishing.org

→ We think you meant to go to: PayPal (paypal.com)
Warning—Suspected phishing page!

This page may be a forgery designed to trick you into sharing sensitive information. Entering any information here may result in identity theft or other abuse.

→ What is phishing and how do I protect myself? Click to learn more: antiphishing.org

→ We think you meant to go to: PayPal (paypal.com)

Back to Safety

escape #1
Warning—Suspected phishing page!

This page may be a forgery designed to trick you into sharing sensitive information. Entering any information here may result in identity theft or other abuse.

→ What is phishing and how do I protect myself? Click to learn more: antiphishing.org

→ We think you meant to go to: PayPal (paypal.com)

Back to Safety

escape #2
challenges
extensions = effort
this works
stopped class of attacks
AuntieTuna

effective and usable
use it, hack it

https://ant.isi.edu/software/antiphish