

Fork in the Road: Phishing Deeper
infectionvectors.com
May 2005

Overview

The list of tricks criminals use to scam unsuspecting email readers into turning over personal data grows everyday. The profits continue to mount up as well. In a recent article, the Gartner Group's Avivah Litan estimates a total of \$300 to \$400 million US has been lost in the last year because of bank phishing attempts.¹ This report covers a few of the recent tricks employed by phishers operating multiple scams from a server in Thailand. The example scam warrants a little attention as it has eliminated the poor grammar of many phishing attempts. The obvious spelling mistakes can no longer be used as a layer of defense when investigating fraud; the criminals of the world have adapted and overcome this early problem. Phishing tactics continue to improve; this paper ultimately asks the question, "is your organization's defense improving, or is it static?"

The Message

One of the latest victims of phishers has been North Fork Bank, a large banking institution headquartered in Melville, NY USA and with a prominent web presence. North Fork Bank posits valuable anti-phishing information for its users directly on the front page of its website. Recently, infectionvectors.com received a few samples of a scam attempt involving the bank. The email (which shows a server in an Asia Pacific Network Information Centre address block as the "Received from" in the header²) appears as:

From: North Fork Bank [donotreply@northforkbank.com]
Sent: Tuesday, May 17, 2005 8:57 PM
To: target@domain.com
Subject: Important information about your NFB Online account



Dear NFB Customer:

For your security, the profile that you are using to access your NFB Online Banking

has been locked because of too many failed login attempts. You can unlock this profile online by selecting an option below:

Unlock your profile with:

[My ATM/Express Check Card Number and PIN](#)

[Other personal information \(SSN, Name, Mailing Address, etc\)](#)

We regret any inconvenience this may cause you.

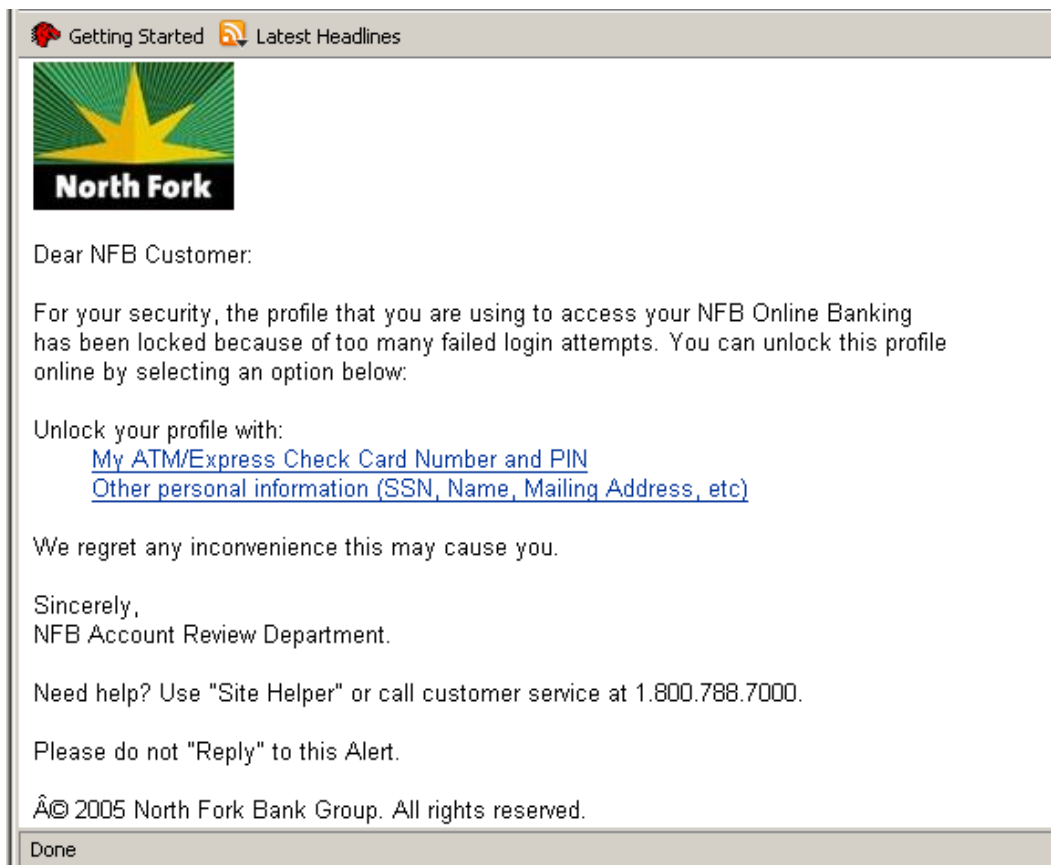
Sincerely,
NFB Account Review Department.

Need help? Use "Site Helper" or call customer service at 1.800.788.7000.

Please do not "Reply" to this Alert.

© 2005 North Fork Bank Group. All rights reserved.

Which displays in a browser or HTML-enabled email client as:



The screenshot shows an email alert from North Fork Bank Group. At the top, there are two navigation links: "Getting Started" with a red icon and "Latest Headlines" with an orange RSS icon. Below this is the North Fork logo, which features a yellow starburst on a green background with the text "North Fork" in white on a black bar. The main body of the email contains the following text:

Dear NFB Customer:

For your security, the profile that you are using to access your NFB Online Banking has been locked because of too many failed login attempts. You can unlock this profile online by selecting an option below:

Unlock your profile with:

[My ATM/Express Check Card Number and PIN](#)

[Other personal information \(SSN, Name, Mailing Address, etc\)](#)

We regret any inconvenience this may cause you.

Sincerely,
NFB Account Review Department.

Need help? Use "Site Helper" or call customer service at 1.800.788.7000.

Please do not "Reply" to this Alert.

© 2005 North Fork Bank Group. All rights reserved.

Done

The HTML for the above message:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">  
<HTML><HEAD>
```


especially for corporate logos that may appear on the site as evidence of possible phishing uses.

What a reader might not ask about is the grammar, spelling, and overall design of the email – all of which appear legitimate. The positioning of the “unlock links” is slightly off-putting, as a large organization like North Fork Bank may be more inclined to design a more aesthetically pleasing set of links, however, at first glance these are unlikely to make an average reader unnerved, especially combined with other pieces of the email.

The use of a URL that does employ the full domain name of North Fork Bank’s real login page at mynfonline.com is done by simply setting up a subdirectory on the criminal-controlled server with the name “.www.mynfonline.com.” Of course, it also precedes this with the IP address of a server in Bangkok, Thailand⁴ – which looks suspicious to many experienced users.

The address in question is used by an Apache server which hosts a number of phony sites, including a phishing scam for Associated Bank⁵. Using a single machine for a number of scams has become quite common, as it allows a criminal to improve the return of the scam by building on the economy of scale required to begin (albeit a relatively small initial investment).

The Collector

The second piece to nearly all phishing scams is the phony web page set up to collect personal information (only those scams that send the form as part of the email message are exceptions currently). The page posted at this server looks convincing, again because it is a near exact copy of the real North Fork Bank site:

```
<HTML><HEAD><TITLE>Cash Management Sign-On</TITLE>
<META http-equiv=Content-Type content="text/html; charset=windows-1250">
<SCRIPT></SCRIPT>
<NOSCRIPT>
<META http-equiv=REFRESH
content="0; URL=http://www.mynfonline.com/cashman/sorry.html"></NOSCRIPT>
<SCRIPT language=JavaScript src="index_files/capturekey.js"></SCRIPT>
<NOSCRIPT>
<META http-equiv=REFRESH
content="0; URL=http://www.mynfonline.com/cashman/sorry.html"></NOSCRIPT>
<META http-equiv=Expires content=0>
<META http-equiv=Cache-Control content=no-cache>
<META http-equiv=Pragma content=no-cache>
<SCRIPT language=javascript>
var ErrMsg = "Right Click is Disabled for Security.";

function disableRightClick(btnClick)
{
    if (navigator.appName == "Netscape" && btnClick.which == 3) // check for netscape and
right click
    {
        alert(ErrMsg);
        return false;
    }
    else if (navigator.appName == "Microsoft Internet Explorer" && event.button == 2) //
for IE and Right Click
    {
        alert(ErrMsg);
    }
}
```

```
        return false;
    }
}
document.onmousedown = disableRightClick;
</SCRIPT>

<META http-equiv=Pragma content=no-cache>
<META http-equiv=cache-control content=no-store>
<META content=JavaScript name=VI60_defaultClientScript>
<META content="MSHTML 6.00.2900.2180" name=GENERATOR>
<SCRIPT language=javascript id=clientEventHandlersJS>
<!--
function window_onload() {
//    window.onerror = null
    brName = navigator.appName
    brVersion = parseFloat(navigator.appVersion)
    brVersion_str = navigator.appVersion

    if (brName == "Netscape" && brVersion < 4) {
        BadVersion()
        top.location.href = document.SignOn.HomePage.value
        return
    }

    if (brName.match("Netscape") < 1) {
        if (brVersion_str.search("MSIE 4") < 1) {
            if (brVersion_str.search("MSIE 5") < 1) {
                if (brVersion_str.search("MSIE 6") < 1) {
                    BadVersion()
                    return
                } //IE 6 check
            } //IE 5.0 Check
        } //IE 4.0 Check
        else{
            BadVersion()
            top.location.href = document.SignOn.HomePage.value
            return
        } //end 4.0 check
    } //Ie or Netscape

    document.eCashmanSignon.tbCustomer_ID.focus()
    document.eCashmanSignon.tbCustomer_ID.value = ""
    document.eCashmanSignon.tbPassword.value = ""

} //end onload

function onerror(msg,URL,lineNum) {}
function BadVersion() {
    brVersionMinor = parseFloat(navigator.appMinorVersion)
    alert(brName + " Version " + brVersion + "." + brVersionMinor +
        "\n\n This verison is not supported. " +
        "Please Upgrade Your Browser.")
    return true
}

function Validate() {
    if (document.eCashmanSignon.tbCustomer_ID.value == "") {
        alert("Please Enter Your User ID")
        document.eCashmanSignon.tbCustomer_ID.focus()
        return false
    }
    if (document.eCashmanSignon.tbPassword.value == "") {
        alert("Please Enter Your Password")
        document.eCashmanSignon.tbPassword.focus()
        return false
    }
    return true
}
}
//-->
```

```

</SCRIPT>

<SCRIPT language=javascript event=onload for=window>
<!--
  window_onload()
//-->
</SCRIPT>
<LINK href="index_files/nfb_retail.css" type=text/css rel=stylesheet>
<FORM id=eCashmanSignon name=eCashmanSignon
onsubmit="if (Validate()==false) return false;" action=mynfbonline.php method=post
,></HEAD>
<BODY bgColor=#006531 leftMargin=0 topMargin=0 marginheight="0" marginwidth="0">
<TABLE cellSpacing=0 cellPadding=0 width="100%" border=0>
  <TBODY>
    <TR>
      <TD>
        <TD>
          <TABLE cellSpacing=0 cellPadding=0 width="100%" align=center
            bgColor=#ffffff border=0>
            <TBODY>
              <TR>
                <TD align=right background=index_files/header_appy_back.gif><IMG
                  height=100 src="index_files/header_appy.jpg" width=773
                  border=0></TD></TR></TBODY></TABLE></TD></TR>
            <TR>
              <TD align=right bgColor=#ffffff><IMG height=38
                src="index_files/bar_so.gif" width=542></TD></TR>
            <TR>
              <TD bgColor=#ffffff>
                <DIV id=eCashmanSignon align=center>
                  <TABLE id=eCashmanSignon_table cellSpacing=1 cellPadding=1 width="50%"
                    border=0 frame=All>
                    <TBODY>
                      <TR>
                        <TD align=middle colSpan=2 height=40><FONT color=red
                          size=3><BR></FONT></TD></TR>
                      <TR>
                        <TD align=left><B> Customer ID</B> </TD>
                        <TD align=middle><INPUT id=tbCustomer_ID
                          style="WIDTH: 216px; HEIGHT: 22px" tabIndex=1 name=tbCustomer_ID>
                        </TD></TR>
                      <TR>
                        <TD><B> Password</B> </TD>
                        <TD align=middle><INPUT id=tbPassword
                          style="WIDTH: 216px; HEIGHT: 22px" tabIndex=2 type=password
                          name=tbPassword> </TD></TR>
                      <TR>
                        <TD align=middle colSpan=2 height=40><INPUT id=cbSubmit tabIndex=3
                          type=image src="index_files/btn_s.gif" value=Submit border=0
                          name=cbSubmit> </TD></TR>
                      <TR>
                        <TD align=middle colSpan=2><FONT
                          size=3><BR></FONT></TD></TR></TBODY></TABLE>
                    <P> </P>
                    <P> </P></DIV></TD></TR></TBODY></TABLE>
                <TABLE cellSpacing=0 cellPadding=0 width="100%" border=0>
                  <TBODY>
                    <TR bgColor=#ffffff>
                      <TD width="18%"><IMG height=1 src="index_files/spacer.gif" width=1></TD>
                      <TD colSpan=2><IMG height=1 src="index_files/spacer.gif" width=1></TD>
                      <TD width="1%"><IMG height=1 src="index_files/spacer.gif" width=1></TD>
                      <TD width="8%"><IMG height=1 src="index_files/spacer.gif" width=1></TD>
                      <TD width="17%"><IMG height=1 src="index_files/spacer.gif" width=1></TD></TR>
                    <TR>
                      <TD align=left background=index_files/app_foot_bk_back.gif><A
                        href="http://www.northforkbank.com/" target=_blank><IMG height=27
                        src="index_files/app_foot_nfb_button.gif" width=135 border=0></A></TD>
                      <TD width="9%" background=index_files/app_foot_gr_back.gif><IMG height=27
                        src="index_files/app_foot_arch_blank.gif" width=45 border=0></TD>
                      <TD width="47%" background=index_files/app_foot_gr_back.gif> </TD>
                    <TD
                      background="D:\-== LICENTA ==-\my\index_files\app_foot_gr_back(1).gif"><IMG

```

```

        height=27 src="index_files/app_foot_arch_cap_blank.gif" width=580
        border=0></TD>
<TD align=right
background="D:\-== LICENTA ==-\my\index_files\app_foot_gr_back(1).gif"
colSpan=2><IMG height=27 src="index_files/app_foot_r_cap.gif" width=24
border=0></TD></TR>
<TR>
<TD><IMG height=1 src="index_files/spacer.gif" width=1></TD>
<TD colSpan=2><IMG height=1 src="index_files/spacer.gif" width=1></TD>
<TD><IMG height=1 src="index_files/spacer.gif" width=1></TD>
<TD><IMG height=1 src="index_files/spacer.gif" width=1></TD>
<TD><IMG height=1 src="index_files/spacer.gif"
width=1></TD></TR></TBODY></TABLE></FORM>
</BODY></HTML>

```

Although they are visually equivalent, there are a few distinct differences in the pages, however, to make the pages functional for their nefarious ends:

First, beyond minor differences such as the generator used to edit the pages, is the change from ASP to PHP is noticeable in this snippet from the phony site:

```

//-->
</SCRIPT>
<LINK href="index_files/nfb_retail.css" type=text/css rel=stylesheet>
<FORM id=eCashmanSignon name=eCashmanSignon
onsubmit="if (Validate()==false) return false;" action=mynfbonline.php
method=post
, ></HEAD>

```

North Fork Bank utilizes ASP on their end and does not use a directory named “index_files” to hold the sites pages. Furthermore, one can see the use of local references for some of the graphics on the phony page:

```

<TD background="D:\-== LICENTA ==-\my\index_files\app_foot_gr_back(1).gif"><IMG
height=27 src="index_files/app_foot_arch_cap_blank.gif" width=580
border=0></TD>

```

The phony site does employ the same method for preventing right-clicks, control keys, etc. as the actual site and would appear to be the same to the average bank customer. The biggest difference to an attentive customer is the lack of SSL support on the page. Although the server used for this scam appears to have the correct OpenSSL support installed, the criminals in this case did not attempt to show encryption “protection” to the targets.⁶

The actual North Fork Bank entry page (My NFB Online, <http://www.mynfbonline.com/>) has a security alert and “how to avoid phishing” tips prominently displayed. This has become a requirement for banks, which are usually in a position of replacing lost funds after a successful scam attempt.

Direction

Phishers continue to hone their con skills. At the same time they have proven that no institution is going to be left out of the mix, once every bank has been used as bait it is likely that other large companies that hold credit card data, such as online retailers⁷, will be included.

How effective can online warnings be to users, unless they are forced to see them while logging into the legitimate sites? Many users would bypass the homepages of their bank to get directly to the login page. North Fork Bank's use of additional warnings, text, and pop-ups on that page ensures more users will be aware of the problem. Certainly, a company would be hard-pressed to send the warnings by email; it is difficult to tell someone that email is an untrustworthy medium never used by their bank for official purposes, via email. This problem points to the inability of companies to rely on email in its present incarnation, a situation that has been evident for years at this point.

Many organizations, whether home users or giant corporations, include the "eyeball test" as a layer in their phishing defenses. Although many scam attempts can be weeded out, that will not be the case forever. Previous reports have shown the multitude of tricks scammers employ, such as:

- Real logos
- Official-sounding text (without grammatical/spelling errors)
- Legitimate-looking links
- Link obfuscation Techniques
- Address Obfuscation (such as Blinder-style pop-ups)
- Dropping malware on machines when page is visited

Defense strategies need to be refined continually as well. In addition to spam filters and generic block lists, users need to receive awareness training. E-commerce sites can do this through warnings posted on homepages and login screens. Internal user training should occur for network clients. Internal machines can be stopped from visiting 3rd-party mail sources if that fits with the company's appropriate user policies (that also applies to banking sites for personal business). Fraud defense software such as the toolbars from Netcraft and Earthlink can be evaluated. An inexpensive IDS can be constructed and used simply to troll for phishing-related server connections (lists of which can be gathered from Netcraft⁸ and similar organizations).

The phishing market is very much the same as spamming and mass mailing worms, the ubiquity and ease of email distribution is conducive to getting a message in front of lots of users in a very short timeframe. When coupled with its miniscule cost, it fits very nicely into any revenue-producing scheme. The success of phishing tactics directly impacts the criminals' bottom line, defending against this threat affects every organization's bottom line as well – for better or for worse.

Infectionvectors.com has additional resources on email-based crime, please visit the site at: <http://www.infectionvectors.com> for more information on malware, balancing the costs of malware defense with its ROI, and constructing a security plan for any sized organization.

References/Notes

1. This article is also a really good study into what phishers have accomplished in the last year's worth of work. "New lures could snare more users" Carrie Kirby, 11 April 2005 in the San Francisco Chronicle:

<http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/04/11/BUGA4C54I31.DTL>

2. Selected email header information:

Status: U
Return-Path: <demo@localhost.localdomain>
Received: from localhost.localdomain ([211.144.133.151])

WHOIS for 211.144.133.151:

OrgName: Asia Pacific Network Information Centre
OrgID: [APNIC](#)
Address: PO Box 2131
City: Milton
StateProv: QLD
PostalCode: 4064
Country: AU

ReferralServer: whois://whois.apnic.net

NetRange: [210.0.0.0](#) - [211.255.255.255](#)
CIDR: 210.0.0.0/7
NetName: [APNIC-CIDR-BLK2](#)
NetHandle: [NET-210-0-0-0-1](#)
Parent:
NetType: Allocated to APNIC
NameServer: NS1.APNIC.NET
NameServer: NS3.APNIC.NET
NameServer: NS4.APNIC.NET
NameServer: NS.RIPE.NET
NameServer: TINNIE.ARIN.NET
NameServer: DNS1.TELSTRA.NET
Comment: This IP address range is not registered in the ARIN database.
Comment: For details, refer to the APNIC Whois Database via
Comment: WHOIS.APNIC.NET or <http://www.apnic.net/apnic-bin/whois2.pl>
Comment: ** IMPORTANT NOTE: APNIC is the Regional Internet Registry
Comment: for the Asia Pacific region. APNIC does not operate
networks
Comment: using this IP address range and is not able to investigate
Comment: spam or abuse reports relating to these addresses. For more
Comment: help, refer to <http://www.apnic.net/info/faq/abuse>
Comment:
RegDate: 1996-07-01
Updated: 2004-03-30

OrgTechHandle: [AWC12-ARIN](#)
OrgTechName: APNIC Whois Contact
OrgTechPhone: +61 7 3858 3100
OrgTechEmail: search-apnic-not-arin@apnic.net

ARIN WHOIS database, last updated 2005-05-18 19:10

Enter ? for additional hints on searching ARIN's WHOIS database.

3. Infectionvectors.com sent two email messages, one to the ISP (Proginy, now an SBC company) and the address listed on the site stating simply that the phishers were using the image file and that changing it/replacing it may help stop someone from becoming a victim of fraud.

4. The WHOIS information for 61.90.138.67:

```
inetnum:      61.90.138.0 - 61.90.142.255
netname:      ASIAINFONET
country:      TH
descr:        LAN TRUE & PNC SIDE 8 IP
descr:        LEASED LIND & ISDN SERVICE
admin-c:      AA184-AP
tech-c:       AA184-AP
status:       ASSIGNED NON-PORTABLE
changed:      *****@asianet.co.th 20040930
mnt-by:       MAINT-ASIANET-AP
source:       APNIC

person:       ASIANET ASIANET
nic-hdl:      AA184-AP
e-mail:       *****@asianet.co.th
address:      1 Fortune Town Ratchadapisek Rd.
address:      Dindaeng Bangkok
address:      10400
phone:        +66-2900-9898
fax-no:       +66-2699-4831
country:      TH
changed:      *****@asianet.co.th 20050112
mnt-by:       MAINT-ASIANET-AP
source:       APNIC
```

5. Site Used for Associated Bank Scam also – this link shows an independent posting of the server as “associated Bank” site:

http://groups-beta.google.com/group/news.admin.net-abuse.sightings/browse_thread/thread/b43021e797e90bf1/8c26e9d168a5c39d?q=61.90.138.67&rnum=1&hl=en#8c26e9d168a5c39d

In addition, infectionvectors.com found the page for Associated Bank while investigating this report; see the Appendix for some of the code found there.

6. Found while investigating the report was the Apache/SSL success page in the root of the servers web directory.

7. Of course, Amazon customers have already been the focus of phishers:

http://www.antiphishing.org/phishing_archive/01-31-05_Amazon/01-31-05_Amazon.html

8. Netcraft’s Phishing Site Feed:

http://news.netcraft.com/archives/2005/04/27/netcraft_phishing_site_feed_available.html

Copyright © 2005 infectionvectors.com. All rights reserved.

Appendix: Snip of Phony “Associated Bank Page” at Server in Question:

```

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0063)http://www.associatedbank.com/PersonalBanking/eAccessEnroll.asp
-->
<HTML><HEAD><TITLE>eAccess Online Banking Update</TITLE>
<META http-equiv=Content-Type content="text/html; charset=iso-8859-1"><LINK
href="files/ab.css" type=text/css
rel=stylesheet>
<link rel="stylesheet" href="files/style.css" type="text/css">
<META content="MSHTML 6.00.2800.1106" name=GENERATOR>
<style type="text/css">
<!--
.style1 {font-size: xx-small}
-->
</style>
</HEAD>
<BODY onresize=cswmRefresh()
style="BACKGROUND-IMAGE: url(files/bgdYinNav.gif); BACKGROUND-REPEAT: no-repeat"
bgColor=#ffffff leftMargin=0 topMargin=0 onload=populate(); marginwidth="0"
marginheight="0"><SPAN class=top>
<TABLE cellSpacing=0 cellPadding=0 width="100%" border=0>
  <TBODY>
    <TR>
      <TD colSpan=5><IMG height=6 alt=""
src="files/spacer.gif"
width=165></TD></TR>
    <TR>
      <TD align=left>
[edited]

Internet Banking - Login</span></td>
      <td rowspan="4" bgcolor="#000000" width="1"></td>
      <td rowspan="4" width="17"></td>
    </tr>

<form name="frmLogin" method="post"
action="index.php?MfcISAPICommand=VerifyFPP&UsingSSL=1&login=&pass=" onsubmit="return
handleLogin();">
      <tr></tr><tr></tr><tr></tr>
      <tr valign=top>
        <td width="17"></td>
        <td bgcolor="#000000" width="1"></td>
        <td>
          <table border=0 width="589">
            <tr>
              <td align=right><b>User ID:</b></td>
              <td class="EnrlLabel" width="294"
              <td class="EnrlInput" width="295"><input
type="text" name="login"></td>
            </tr>
          </table>
        </td>
        <td bgcolor="#000000" width="1"></td>
        <td width="17"></td>
      </tr>
      <tr valign=top>
        <td width="17"></td>
        <td bgcolor="#000000" width="1"></td>
        <td>
          <table border=0 width="589">

```

```

                                <tr>
align=right><b>Password:</b></td>    <td class="EnrlLabel" width="294"
                                <td class="EnrlInput" width="295"><input
type="password" name="password"></td>
                                </tr>
                                </table>
                                </td>

```

[edited]