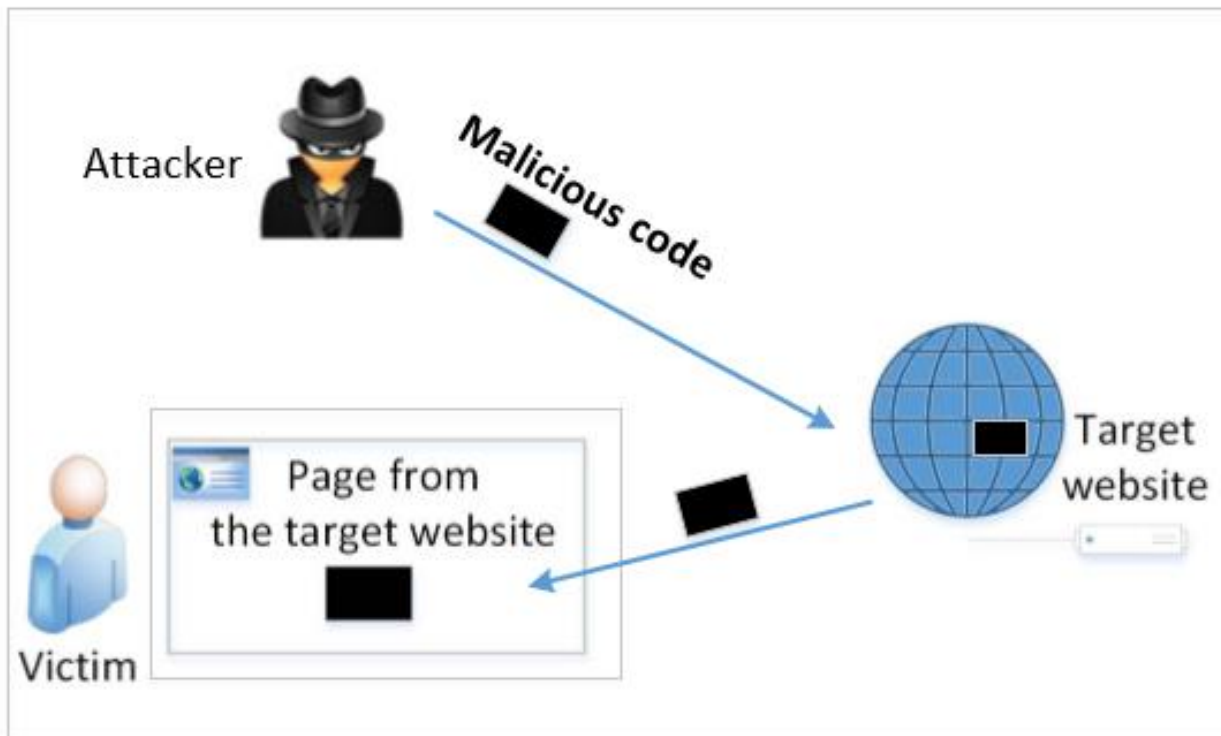


Persistent (Stored) XSS Attack



- Attackers directly send their data to a target website/server which stores the data in a **persistent storage (e.g., Database)**.
- If the website later sends the stored data to other users, the malicious code will be executed **every time**.



Vulnerable HTML page

```
<?php
$Conection_string="host=192.168.1.8 dbname=app user=yyy password=xxx";
$Connect=pg_connect($Conection_string,$PGSQL_CONNECT_FORCE_NEW);

if($_SERVER['REQUEST_METHOD'] == "POST") {
    $query="update $Schema.members set display_name='".$_POST['disp_name']."' where
        user_name='".$_SESSION['USER_NAME']."'";
    pg_query($Connect,$query); }

else {
    if(strcmp($_SESSION['USER_NAME'],'admin')==0) {
        echo "Welcome admin<br><hr>";
        echo "List of user's are<br>";
        $query = "select display_name from $Schema.members where user_name!='admin'";
        $res = pg_query($Connect,$query);
        while($row=pg_fetch_array($res,NULL,PGSQL_ASSOC)) {
            echo "$row[display_name]<br>";  } }

else {
    echo "<form name=\"tgs\" id=\"tgs\" method=\"post\" action=\"home.php\">";
    echo "Update display name:<input type=\"text\" id=\"disp_name\" name=\"disp_name\" value=\"\">";
    echo "<input type=\"submit\" value=\"Update\">"; } }
?>
```

account.php

Update user
table with new
username

Admin views
all user names

Change user
name through
form

https://www.thegeekstuff.com/2012/02/xss-attack-examples/?utm_source=tuicool



How to attack user (or admin)

- Attacker creates submits a username
 - `My Name`
- Username stored in database
- Admin queries all username and clicks the link of the inserted one
- Admin's cookie sent out to attacker's site
 - `http://not-real-xssattackexamples.com`



Countermeasures to Injections

- **Filter and sanitize all user input**
 - Need to account for every potentially valid encoding
 - Make no assumptions about the range of possible user inputs—trust nothing, check everything
- Use access control mechanisms on backend servers, such as “**stored procedures**”
- **HTTP only cookies**
 - Cookies that can only be used in HTTP/HTTPS requests
 - Not accessible by JavaScript via document.cookie



XSS Sanitizers (PHP)

FUNCTION	OUTPUT	DESCRIPTION
<code>intval('123AA456')</code>	123	Sanitize integers. [docs]
<code>filter_var('mark<script>@example.com', FILTER_SANITIZE_EMAIL)</code>	markscript@example.com	Sanitize emails. [docs]
<code>filter_var('Testing <tags> & chars.', FILTER_SANITIZE_SPECIAL_CHARS)</code>	Testing <tags> & chars.	Encode special chars. [docs]
<code>filter_var('Strip <tag> & encode.', FILTER_SANITIZE_STRING);</code>	Strip & encode.	Remove tags. [docs]
<code>filter_var('Strip <tag> & encode.', FILTER_SANITIZE_STRING, FILTER_FLAG_ENCODE_LOW FILTER_FLAG_ENCODE_HIGH FILTER_FLAG_ENCODE_AMP)</code>	Strip & encode.	Remove tags with extra encoding flags. [docs]

<https://www.wordfence.com/learn/how-to-prevent-cross-site-scripting-attacks/#functions-to-escape-and-sanitize-your-data>

HttpOnly Cookies



- Cookie sent over HTTP(s), but not accessible to scripts
 - Cannot be read via document.cookie (JavaScript instruction)
 - Helps prevent cookie theft via XSS



Cross-site Request Forgery (XSRF)

- **Problem:** cookies enable persistent interactions with websites--
- even after you leave them
- **Attack:** malicious websites gets you to perform an operation on a secure site---that you have a **login cookie** for, without your approval



XSRF (cond.)

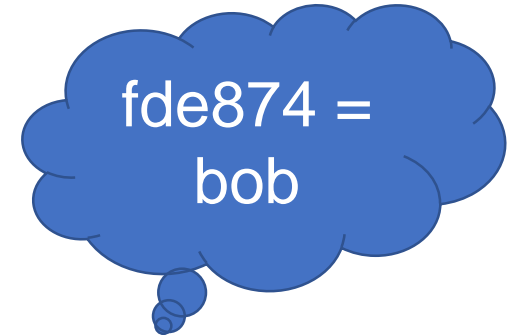
- Root cause: confused about the source of the request
 - Cached credentials is used by browser regardless of who made the request
 - Or “**confused deputy**” problem
- Consider the following common scenario:
 - Alice visits a bank.com, authentication credentials stored
 - 30 minutes later, she accidentally visits a hacker’s site
- **Attack:** malicious site can initiate requests to the bank on Alice’s behalf
 - e.g., attacker may transfer money from Alice’s bank account



XSRF example

- Suppose you log in to bank.com

POST /login?user=bob&pass=abc123 HTTP/1.1
Host: bank.com



bank.com




HTTP/1.1 200 OK
Set-Cookie: login=fde874
....



XSRF example (cond.)

- Suppose you want to see account balance



```
GET /account HTTP/1.1
Host: bank.com
Cookie: login=fde874
```

```
HTTP/1.1 200 OK
....
$378.42
```

fde874 =
bob

bank.com





XSRF example (cond.)

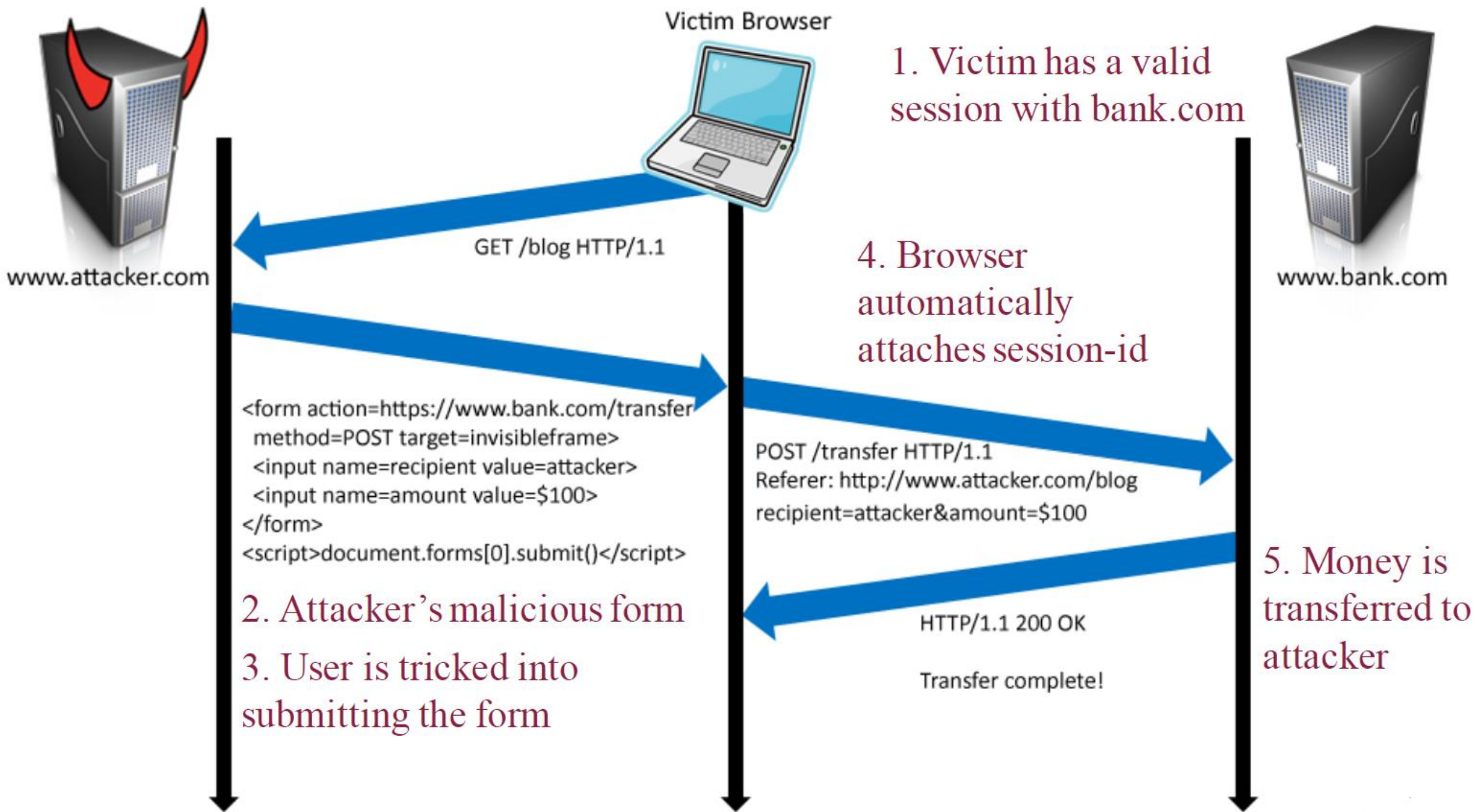
- Attacker trick a victim to visit URL
<http://bank.com/transfer?to=attacker&amt=100>



```
GET /transfer?to=badguy&amt=100 HTTP/1.1
Host: bank.com
Cookie: login=fde874
```

```
HTTP/1.1 200 OK
....
Transfer complete: -$100.00
```







A XSRF Example on reset passwd

- 1. Alice has a valid session with www.mywwwservice.com
- 2. Alice's browser loads page from www.hacker.com
- 3. Evil Script runs causing **evilform** to be submitted with a password-change request to www.mywwwservice.com

```
<form method="POST" name="evilform" target="hiddenframe"
  action="https://www.mywwwservice.com/update_profile">
  <input type="hidden" id="password" value="evilhax0r">
</form>
<iframe name="hiddenframe" style="display: none"> </iframe>
<script>document.evilform.submit();</script>
```

- 4. Browser automatically sends authentication cookies (e.g., session-id, secret keys) along with the request. Alice's password is changed to **evilhax0r**!



XSRF Solutions

- Short-lived credentials
- Delete cookies after transaction
- Add “**referer**” field to HTTP requests
 - Forging referrer may defeat this detection
- Add a **unique identifier (token) to a form**
 - To prevent forms being forged by attackers
- Things that do NOT work
 - Use secret cookies, secret session IDs, encryption,



Anti-XSRF Token

- A server-side XSRF prevention
- Token generation needs to be:
 - Un-guessable, Prevent replay, Support multiple forms, Easy to verify

```
<form action="/transfer.do" method="post">  
  <input type="hidden" name="CSRFToken"  
    value="OWY4NmQwODE4ODRjN2Q2NTlhMmZlYWU...  
    wYzU1YWQwMTVhM2JmNGYxYjJiMGI4MjJjZDE1ZDZ...  
    MGYwMGEwOA=="> ...  
</form>
```



Email security

- Email spam
- Defense



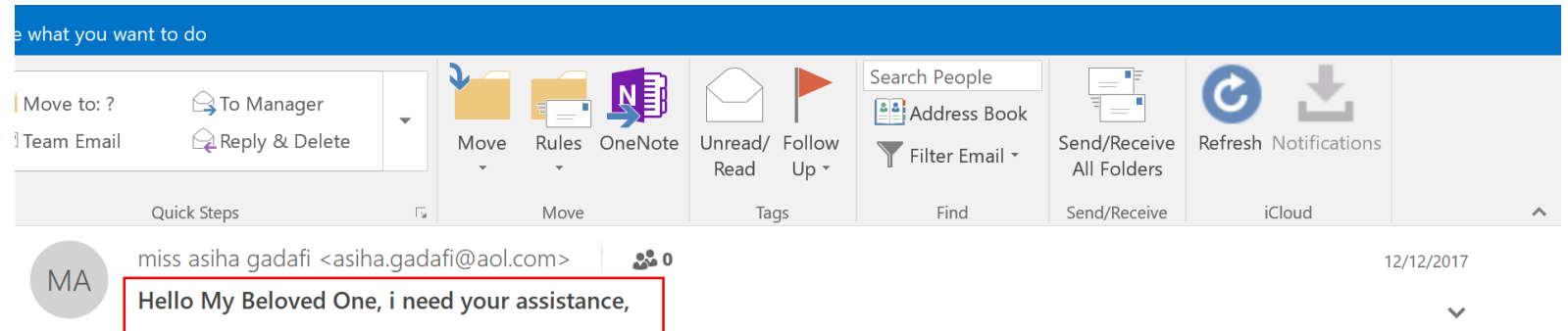
Email Spam

- Definition (informal): emails unwanted/annoying to users
- Experts estimate that **60% to 90%** of all email is spam
- Types of spam:
 - Advertising: pharmaceuticals, fake goods
 - Scam: “Nigerian Prince”
 - Phishing: shipping delivery, account recovery
 - Links for malicious websites
- Spam countermeasures
 - Laws against spam (exist but are generally ineffective)
 - **Email filters** on email servers
 - **Volume limitations** by Internet service providers



Scam

“Nigerian Prince”



Hello My Beloved One, i need your assistance,

Please bear with me i am writing this mail to you with tears and sorrow from my heart.

I am Aisha Muammar Gaddafi, the only daughter of the embattled president of Libya, Hon. Muammar Gaddafi. I know my mail might come to you as a surprise because you don't know me, but due to unsolicited nature of my situation here in Refugee camp Ouagadougou Burkina Faso i decided to contact you for help. I have passed through pains and sorrowful moment since the death of my father. At the meantime, my family is the target of Western nations led by Nato who wants to destroy my father at all costs. Our investments and bank accounts in several countries are their targets to freeze.

My Father of blessed memory deposited the sum of \$5.8M (Five Million Eight Hundred Thousand Dollars) in Africa Develoment Bank (ADB) Burkina Faso which he used my name as the next of kin. I have been commissioned by the (ADB) bank to present an interested foreign investor/partner who can stand as my trustee and receive the fund in his account for a possible investment in his country due to my refugee status here in Burkina Faso.

I am in search of an honest and reliable person who will help me and stand as my trustee so that I will present him to the Bank for the transfer of the fund to his bank account overseas. I have chosen to contact you after my prayers and I believe that you will not betray my trust but rather take me as your own sister or daughter. If this transaction interest you, you don't have to disclose it to any body because of what is going with my entire family, if the united nation happens to know this account, they will freezing it as they freeze others, so please keep this transaction only to yourself until we finalize it.

Sorry for my pictures i will enclose it in my next mail and more about me when i hear from you okay.

Yours Sincerely

Best Regard,

Aisha Gaddafi

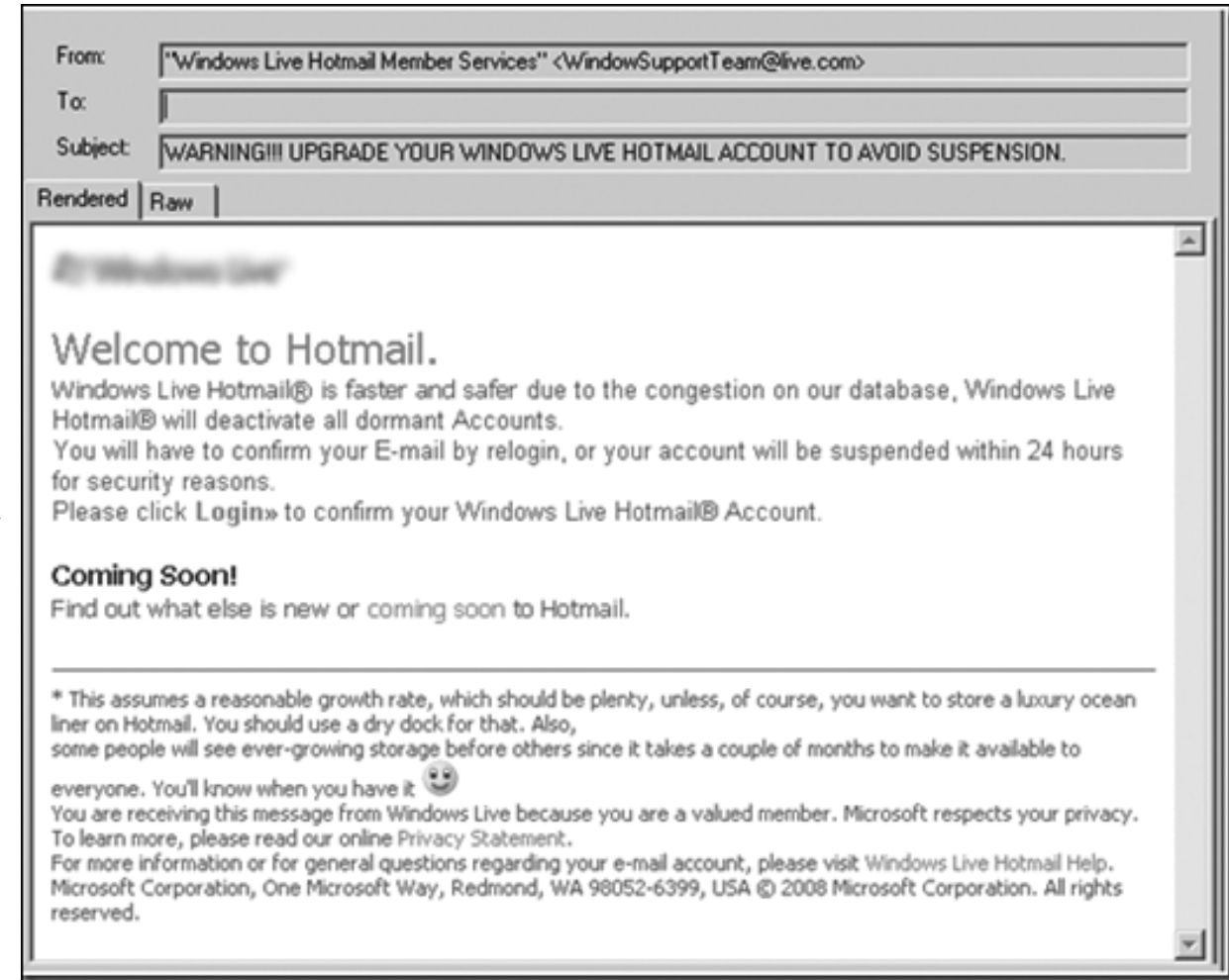
please you can contact me through my private email address(aishag637@gmail.com)





Phishing

- A message that tries to trick a victim into providing private information or taking some other unsafe action
- **Spear phishing**: A targeted attack that is **personalized** to a particular recipient or set of recipients
 - Sponsored by nation-state agencies or competing companies





Email basics

- Three major components:
 - user agents, mail servers, transfer protocol: SMTP
- User agent
 - a.k.a. “mail reader”, e.g., outlook
 - composing, editing, reading mail messages
- Mail Servers
 - Mailbox contains incoming mails for user
 - And message queue of outgoing mails
- SMTP protocol
 - Mail servers to send email messages

