Ethical Student Hackers

Email Security

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

- Relevant UK Law: https://www.legislation.gov.uk/ukpga/1990/18/contents

Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf

Email!

- Used a lot in organisations
- Really old
- Original protocol has effectively no protections
- Impersonation

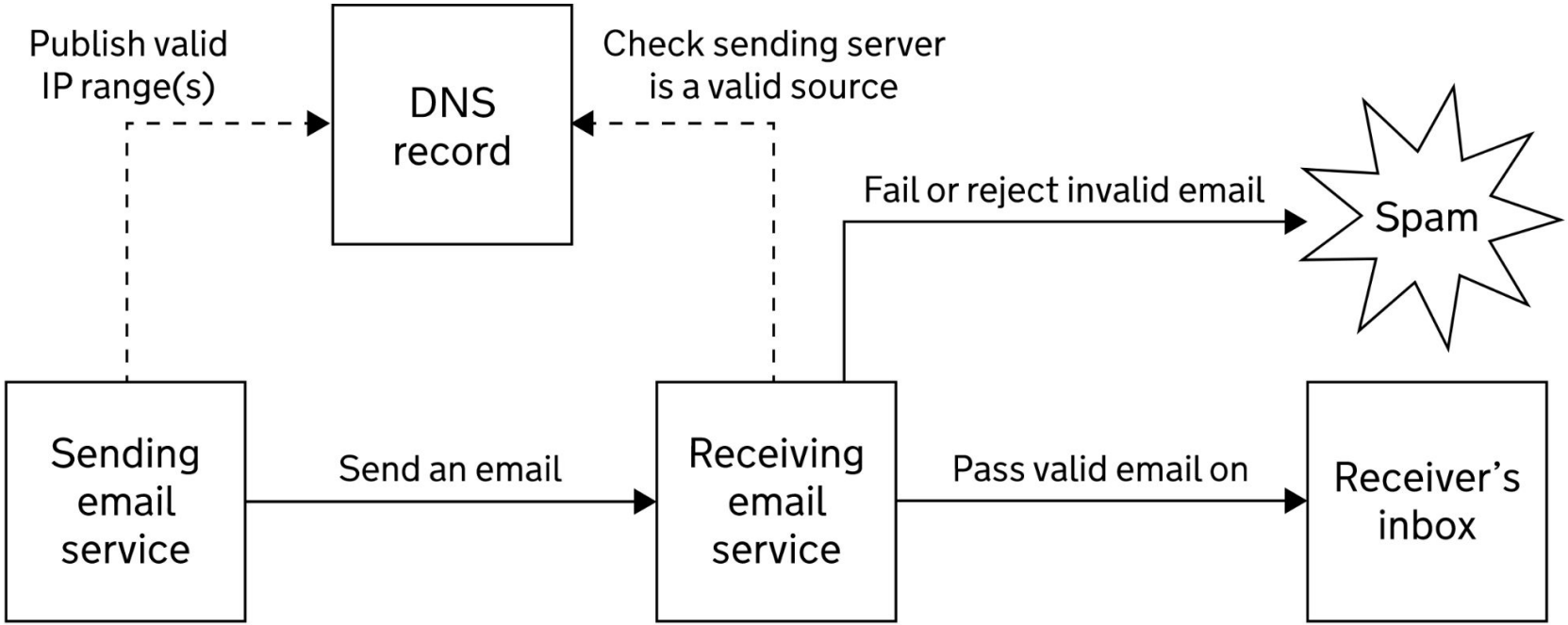
SPF

Sender Policy Framework

1. Source list: mail server IP addresses that a given domain can send mail through
2. Receiving provider checks DNS record
3. Ignores email if source is not found in record

- Need to list any third party email services you use to send legitimate emails from
  - SendGrid
  - Google
  - PostMark

SPF

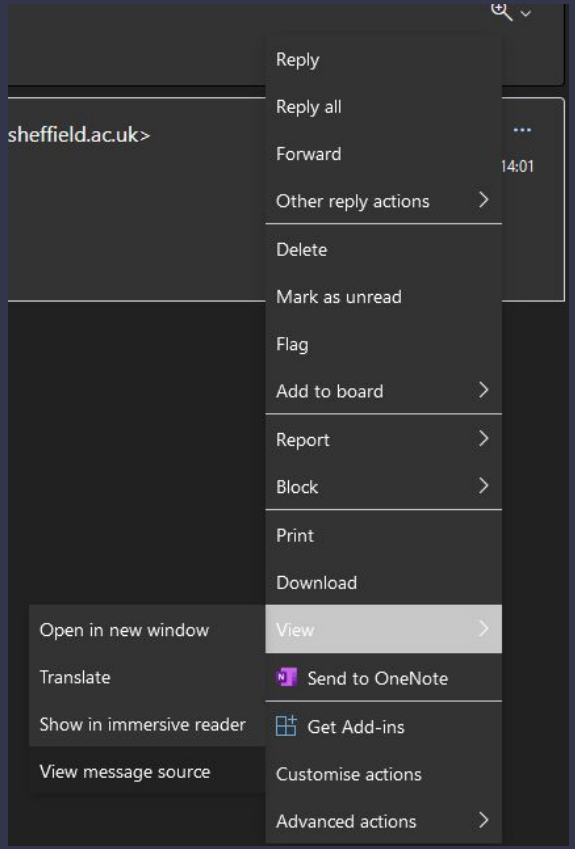


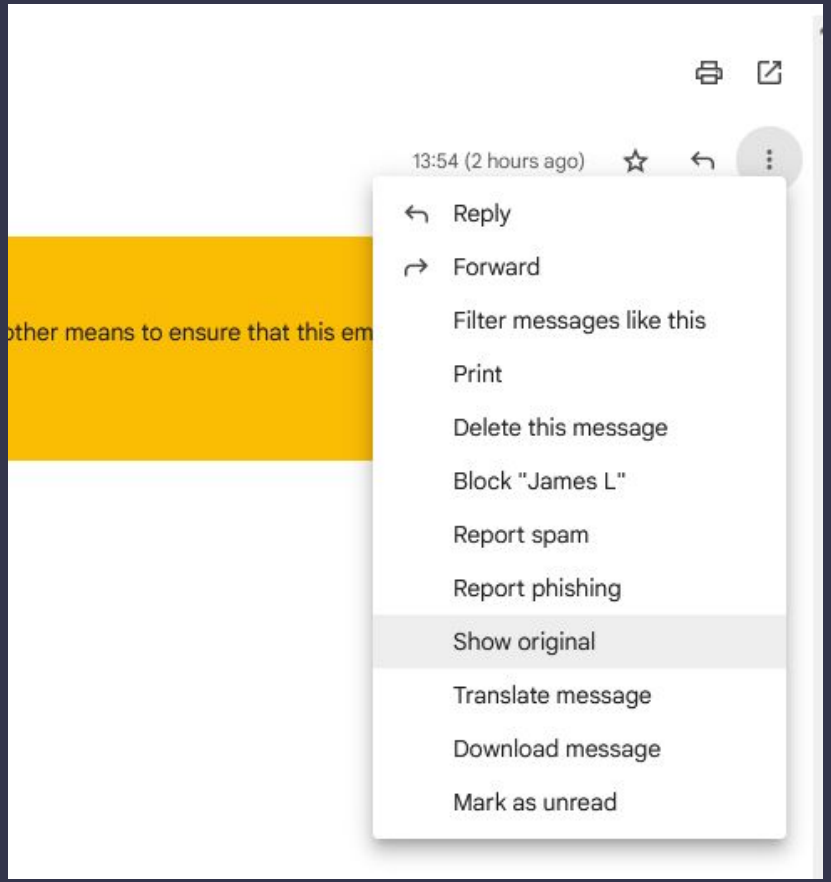
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/image_data/file/83318/govuk-security-diagrams_3.svg

SFP in Action

1. Send an email to a personal email from your Sheffield address.
2. In CMD or Powershell: nslookup -type=txt sheffield.ac.uk
3. View the email source and find the spf check
4. Check the IP address matches those from the record

View Message Source





Results

Partial DNS txt record:
v=spf1 ip4:143.167.0.0/16 ip4:95.172.88.0/22 ip4:130.88.36.5 ip4:80.93.168.194 ip4:85.92.81.226 ip4:146.177.26.90/31 ip4:146.177.26.108/31 ip4:81.17.56.1" " ip4:212.227.126.128/25 ip4:82.165.159.0/26 ip4:212.227.15.0/25 ip4:212.227.17.0/27 ip4:217.72.192.64/26 ip4:74.121.48.4 ip4:31.221.91.141 ip4:212.54.136.59 ip4:31.221.72.237 ip4:35.177.177.249 ip4:35.178.89.45" " include:_spf.google.com include:wpm.flywire.com include:spf.mailanyone.net include:spf.mandrillapp.com include:shops.shopify.com -all

Lists all allowed sources, “-all” means

Client Result:
Received-SPF: Pass (protection.outlook.com: domain of sheffield.ac.uk designates 209.85.167.50 as permitted sender)

Tools

https://mxtoolbox.com/SuperTool.aspx?action=spf

https://mxtoolbox.com/SubnetCalculator.aspx

https://toolbox.googleapps.com/apps/messageheader/ (Doesn't work for all gmail messages despite being google tool)

SPF Syntax

"+" Pass
"-" Fail
"~" SoftFail
"?" Neutral

all: always matches
ip4: ipv4 network range
ip6: ipv6 network range
a: all a records for a domain
mx : all mx records for a domain
include: include spf record of domain
(incomplete, more can be found a link below)

https://web.archive.org/web/20190215111841/http://www.openspf.org/SPF_Record_Syntax

SPF Weaknesses

- Doesn’t ensure message integrity
- Doesn’t protect from field
  - https://web.archive.org/web/20190212011432/http://www.openspf.org/FAQ/Envelope_from_scope
- Overly permissive
  - Has to be setup and mail servers might change
  - Blocks are made two large
  - Scammers get control of an allowed IP
    - https://web.archive.org/web/20240120085716/https://www.welivesecurity.com/2022/08/16/spoofed-email-passed-spf-check-inbox/
  - Why domains are used to manage changes in one place as we saw
- Overwhelm DNS
  - Hides source of attack as receiving server requests
  - However receiving server should limit
  - Traffic also is shrunk (intention is to magnify)

DKIM

DomainKeys Identified Mail

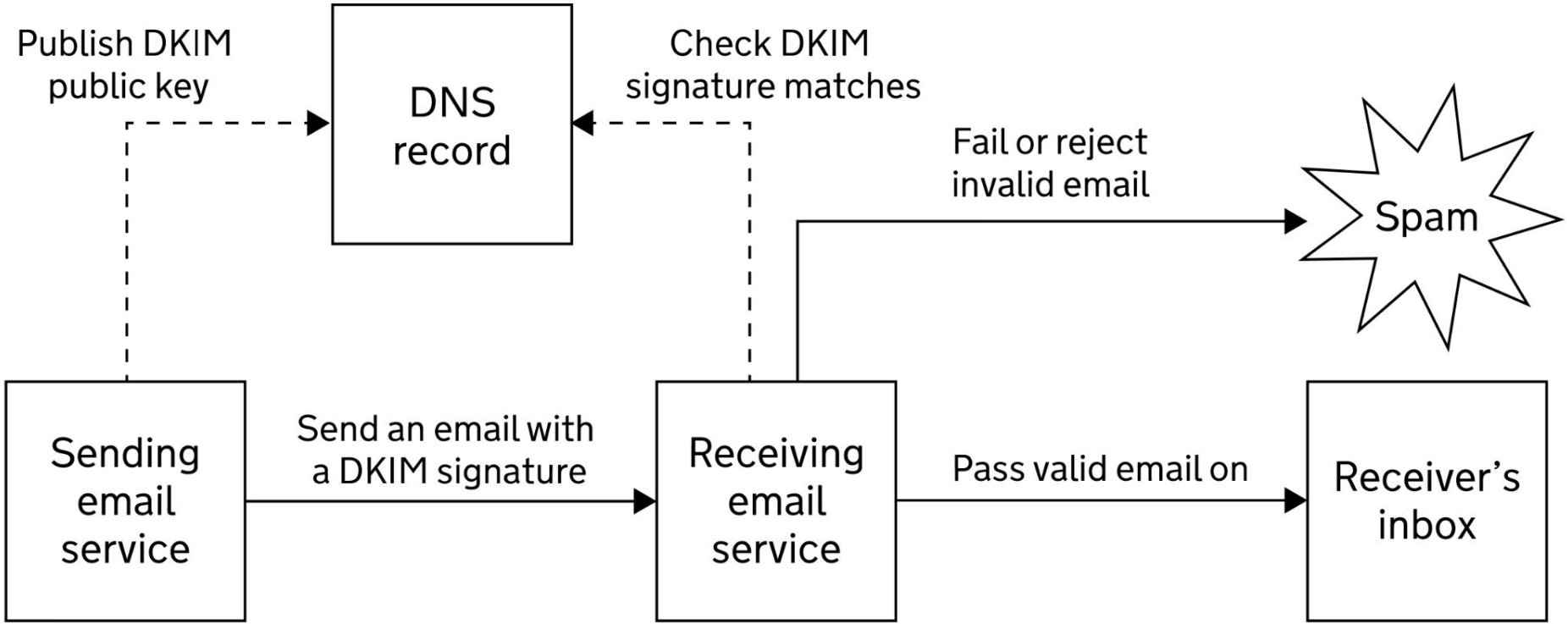
1. Public private key generated
2. Public key stored in source dns record
3. Each email is signed
4. Source verifies the signature was made from the private key (using the public key)
5. Source verifies the signed hash matches the message contents

- Verifies emails domain
- Verifies not been tampered with

DKIM Weaknesses

- Doesn’t encrypt messages
  - Could use PGP
  - Some providers use opportunistic TLS
    - Not good as not completely supported so if it goes through unsupported server will be sent in plain text
- Have keys leak

DKIM



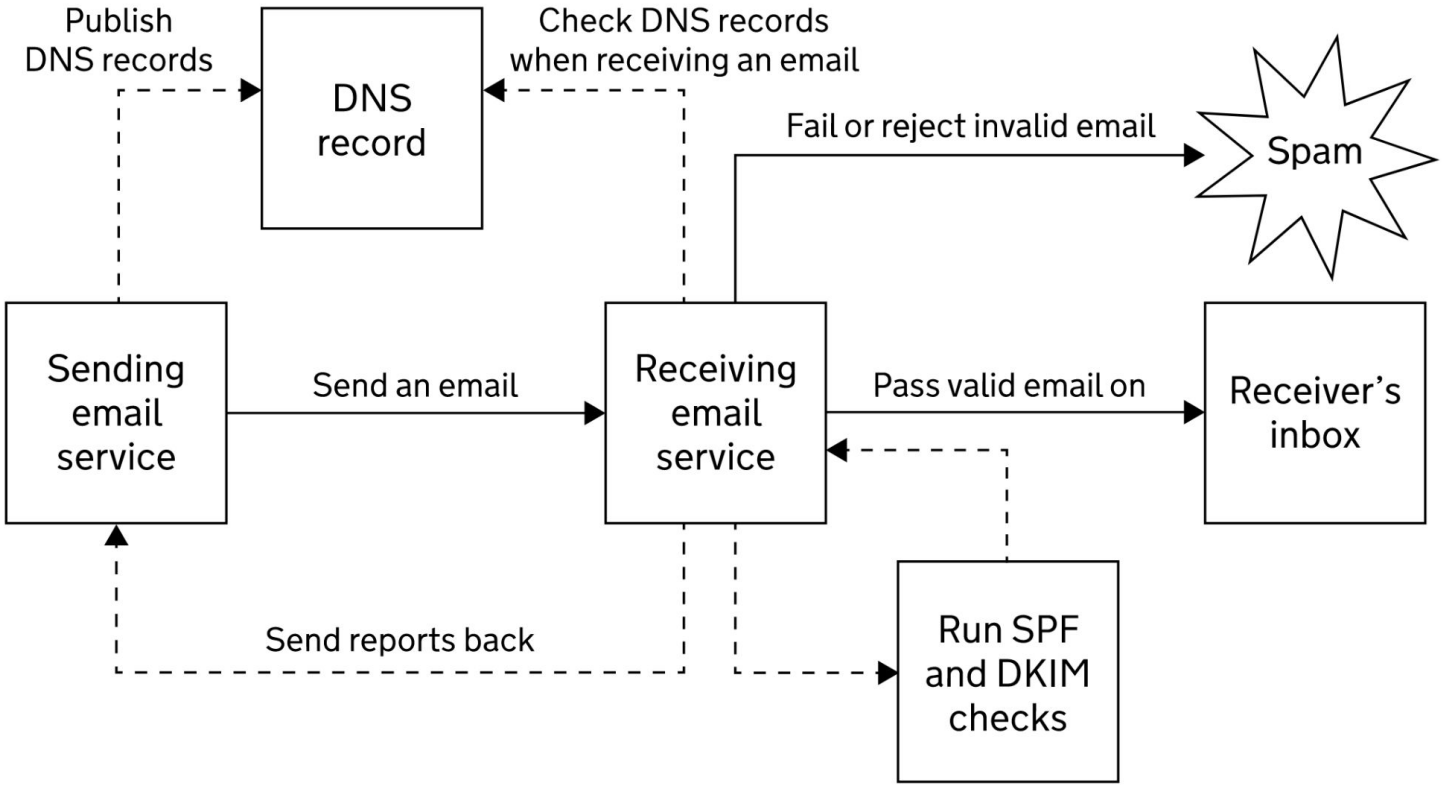
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/image_data/file/83316/govuk-security-diagrams_1.svg

DMARC

Domain-based Message Authentication, Reporting and Conformance

- Uses SPF and DKIM to verify identity
- Policy tells recipient what to do with failed emails
    - Reports allow people to know who is impersonating them

DMARC



https://assets.publishing.service.gov.uk/government/uploads/system/uploads/image_data/file/83311/govuk-security-diagrams_2.svg

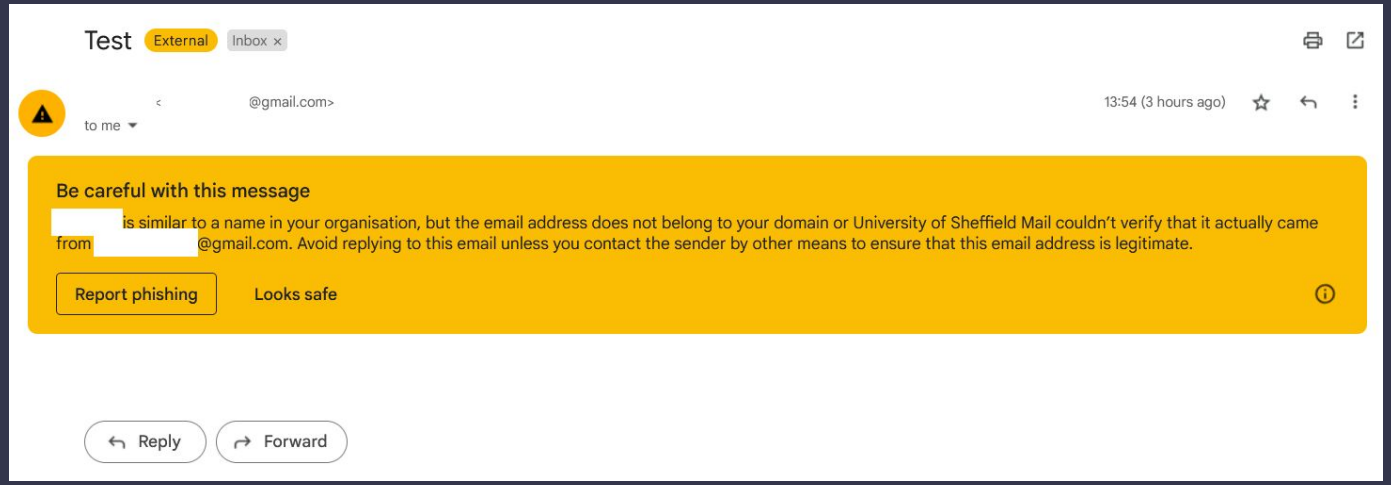
Summary

SPF validates that the server is authorised to send messages using that domain

DKIM ensures messages aren't altered in transit

DMARC instructs receivers how they should deal with unauthenticated emails

Interesting Examples



SPF:	PASS with IP 209.85.220.41 Learn more
DKIM:	'PASS' with domain gmail.com Learn more
DMARC:	'PASS' Learn more

Test forged headers

You can use a tool to send spoofed emails:

https://emkei.cz/

It will send the message but has none of the security features we have discussed.

This will mean that your email provider should give you a warning or completely block it. It may also delay it from your inbox for quite a while.

Interesting Examples

Authentication-Results: spf=none (sender IP is 89.187.129.24) smtp.mailfrom=test.com; dkim=none (message not signed) header.d=none;dmarc=permerror action=none header.from=test.com;compauth=fail reason=001 Received-SPF: None (protection.outlook.com: test.com does not designate permitted sender hosts) Received: from emkei.cz (89.187.129.24) by BN8NAM11FT003.mail.protection.outlook.com (10.13.177.90) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6340.19 via Frontend Transport; Mon, 24 Apr 2023 00:44:57 +0000 X-IncomingTopHeaderMarker: OriginalChecksum:788591708E4F63B348407A81F4409F5F65F79CF9C36314F3B1897013D8BE9470;UpperCasedChecksum:BB0CCF9F519A18C2C645ACD1FF7ECF160A504017E228E7072C34EEC9F31EC673;SizeAsReceived:428;Count:11 Received: by emkei.cz (Postfix, from userid 33) id 4FE029CCE32; Mon, 24 Apr 2023 01:32:11 +0200 (CEST)

Activities

- Try sending an email with a forged from field: https://emkei.cz/ (You may not receive it today if at all, good to see how your provider handles it)
- SPF, DKIM and DMARC assess technical details, the subject and body will also be used to detect spam. Have a go at creating the best spam email you can: https://www.mail-tester.com/

https://github.com/CanIPhish/spf-bypass

Upcoming Sessions

What's up next?

www.shefesh.com/sessions

Any Questions?

www.shefesh.com

Thanks for coming!