

# Computer Security: Communicating with Users

Dr Kami Vaniea

# All sorts of things need to be communicated to users

- Questions – “did you log in from this location?”
- Warnings – “the website has malicious software”
- UI passive indicators – the lock icon on the browser
- Active UI indicators – “You need to generate a key”
- Task-relevant information – “Passwords should be 8 characters long and must have a capital letter.”
- Educational – “10 security behaviors you should do to protect yourself online”

**The goal of today's lecture is how to create useful communications with users on security topics.**

I got this warning when I tried to connect to the internet from a coffee shop.

### Security Alert



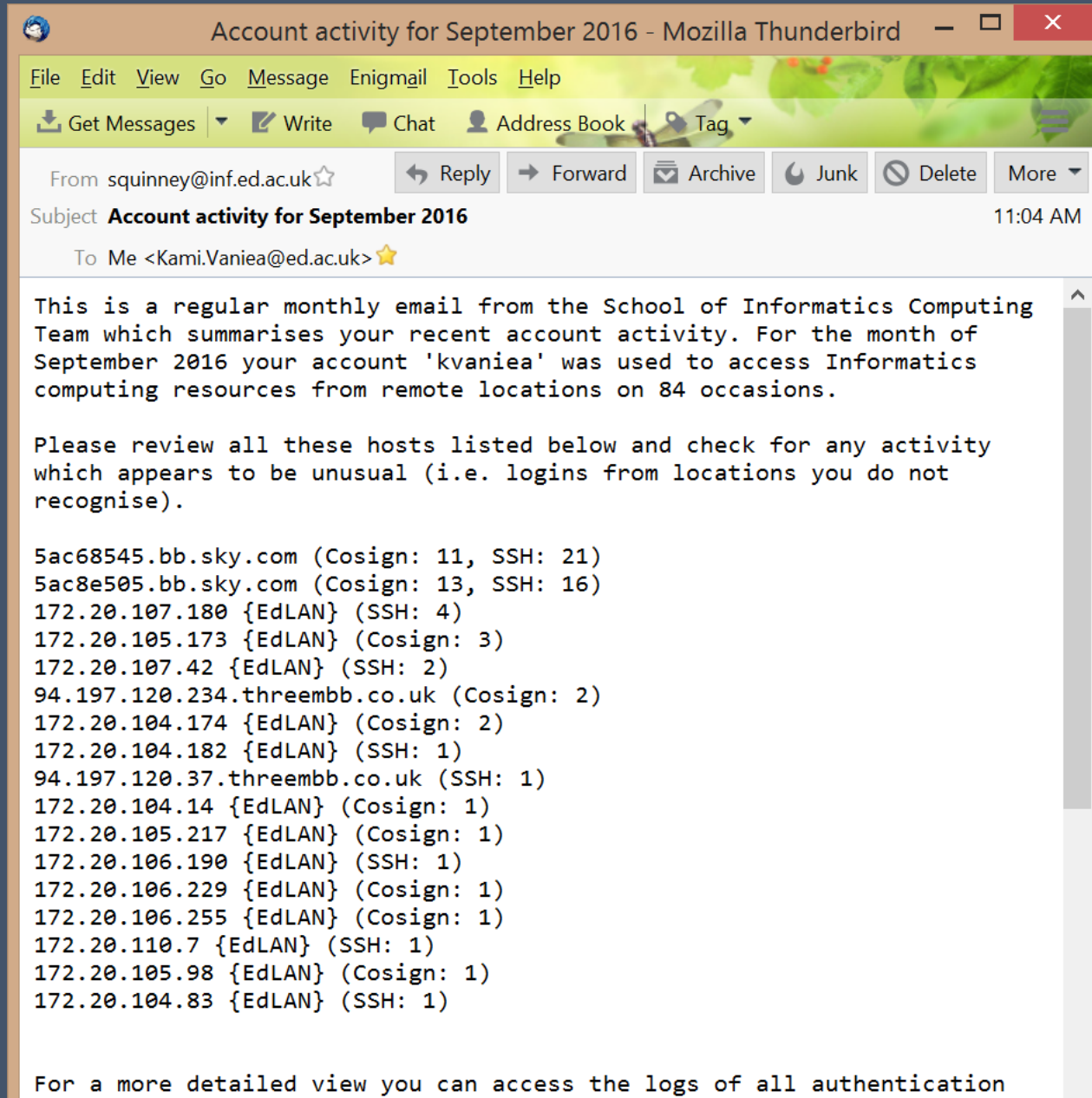
outlook.office365.com

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

- ✓ The security certificate is from a trusted certifying authority.
- ✓ The security certificate date is valid.
- ✗ The name on the security certificate is invalid or does not match the name of the site.

Do you want to proceed?

I get a version of this email every month telling me about all the places I've logged in from.



Account activity for September 2016 - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Get Messages Write Chat Address Book Tag

From squinney@inf.ed.ac.uk ☆ Reply Forward Archive Junk Delete More

Subject **Account activity for September 2016** 11:04 AM

To Me <Kami.Vaniae@ed.ac.uk> ☆

This is a regular monthly email from the School of Informatics Computing Team which summarises your recent account activity. For the month of September 2016 your account 'kvaniea' was used to access Informatics computing resources from remote locations on 84 occasions.

Please review all these hosts listed below and check for any activity which appears to be unusual (i.e. logins from locations you do not recognise).

- 5ac68545.bb.sky.com (Cosign: 11, SSH: 21)
- 5ac8e505.bb.sky.com (Cosign: 13, SSH: 16)
- 172.20.107.180 {EdLAN} (SSH: 4)
- 172.20.105.173 {EdLAN} (Cosign: 3)
- 172.20.107.42 {EdLAN} (SSH: 2)
- 94.197.120.234.threemb.co.uk (Cosign: 2)
- 172.20.104.174 {EdLAN} (Cosign: 2)
- 172.20.104.182 {EdLAN} (SSH: 1)
- 94.197.120.37.threemb.co.uk (SSH: 1)
- 172.20.104.14 {EdLAN} (Cosign: 1)
- 172.20.105.217 {EdLAN} (Cosign: 1)
- 172.20.106.190 {EdLAN} (SSH: 1)
- 172.20.106.229 {EdLAN} (Cosign: 1)
- 172.20.106.255 {EdLAN} (Cosign: 1)
- 172.20.110.7 {EdLAN} (SSH: 1)
- 172.20.105.98 {EdLAN} (Cosign: 1)
- 172.20.104.83 {EdLAN} (SSH: 1)

For a more detailed view you can access the logs of all authentication

# How could we make these two examples more usable?

## Security Alert

outlook.office365.com

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

- ✓ The security certificate is from a trusted certifying authority.
- ✓ The security certificate date is valid.
- ✗ The name on the security certificate is invalid or does not match the name of the site.

Do you want to proceed?

## Account activity for September 2016 - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Get Messages Write Chat Address Book Tag

From squinney@inf.ed.ac.uk

Subject **Account activity for September 2016** 11:04 AM

To Me <Kami.Vaniae@ed.ac.uk>

This is a regular monthly email from the School of Informatics Computing Team which summarises your recent account activity. For the month of September 2016 your account 'kvaniea' was used to access Informatics computing resources from remote locations on 84 occasions.

Please review all these hosts listed below and check for any activity which appears to be unusual (i.e. logins from locations you do not recognise).

```
5ac68545.bb.sky.com (Cosign: 11, SSH: 21)
5ac8e505.bb.sky.com (Cosign: 13, SSH: 16)
172.20.107.180 {EdLAN} (SSH: 4)
172.20.105.173 {EdLAN} (Cosign: 3)
172.20.107.42 {EdLAN} (SSH: 2)
94.197.120.234.threembb.co.uk (Cosign: 2)
172.20.104.174 {EdLAN} (Cosign: 2)
172.20.104.182 {EdLAN} (SSH: 1)
94.197.120.37.threembb.co.uk (SSH: 1)
172.20.104.14 {EdLAN} (Cosign: 1)
172.20.105.217 {EdLAN} (Cosign: 1)
172.20.106.190 {EdLAN} (SSH: 1)
172.20.106.229 {EdLAN} (Cosign: 1)
172.20.106.255 {EdLAN} (Cosign: 1)
172.20.110.7 {EdLAN} (SSH: 1)
172.20.105.98 {EdLAN} (Cosign: 1)
172.20.104.83 {EdLAN} (SSH: 1)
```

For a more detailed view you can access the logs of all authentication

# NEAT and SPRUCE

- Developed at Microsoft Research
- Guidance on how to create effective security messaging for end users

# NEAT

**Necessary** – Can you change the architecture to eliminate or defer this user decision?

**Explained**- Does your user experience present all the information the user needs to make this decision?  
(See SPRUCE)

**Actionable** – Have you determined a set of steps the user will realistically be able to take to make the decision correctly?

**Tested** – Have you checked that your user experience is NEAT for all scenarios, both benign and malicious? Have you tested it on a human who is not a member of your team?

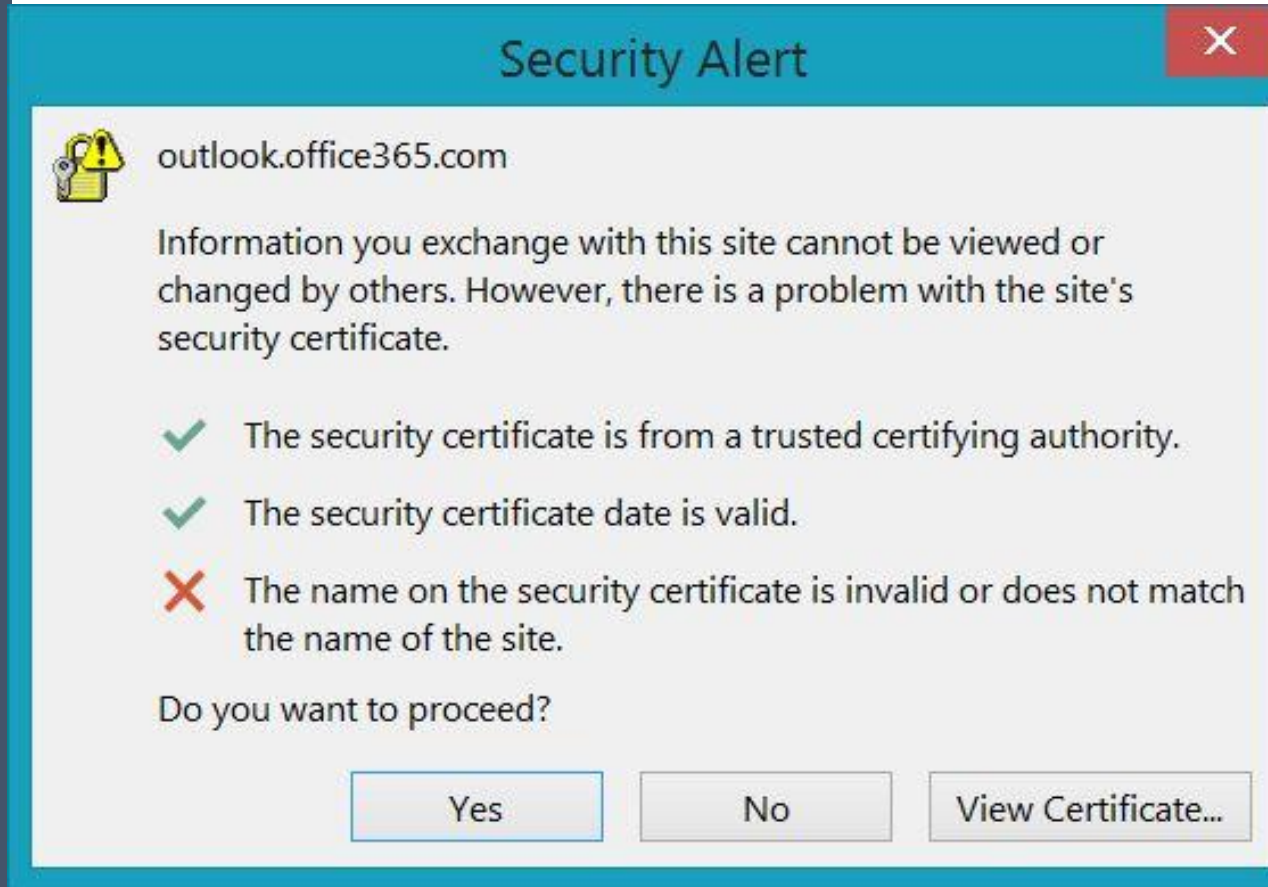


Necessary

Explained

Actionable

Tested



The image shows a Windows-style security alert dialog box. The title bar is teal and contains the text "Security Alert" and a red close button with a white "X". The main content area has a light gray background. At the top left is a yellow warning icon with a black exclamation mark. To its right is the URL "outlook.office365.com". Below this is a paragraph of text: "Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate." This is followed by a list of three items, each with a checkmark or an X icon. The first two items have green checkmarks and describe positive aspects of the certificate. The third item has a red X and describes the problem. At the bottom, the text "Do you want to proceed?" is followed by three buttons: "Yes", "No", and "View Certificate...".

Security Alert

 outlook.office365.com

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

- ✓ The security certificate is from a trusted certifying authority.
- ✓ The security certificate date is valid.
- ✗ The name on the security certificate is invalid or does not match the name of the site.

Do you want to proceed?

Yes No View Certificate...

# SPRUCE

**Source** – State who or what is asking the user to make a decision

**Process** – Give the user actionable steps to follow to make a good decision

**Risk** – Explain what bad thing could happen if they user makes the wrong decision

**Unique** – Knowledge the user has – Tell the user what information they bring to the decision

**Choices** – List available options and clearly recommend one

**Evidence** – Highlight information the user should factor in or exclude in making a decision

Source


Process

Risk

Unique

Choices

Evidence



A screenshot of a Windows Security Alert dialog box. The title bar is teal and contains the text "Security Alert" and a red close button with a white "X". The main content area is white and features a yellow warning icon with a black exclamation mark and a padlock. To the right of the icon is the text "outlook.office365.com". Below this, a paragraph of text reads: "Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate." This is followed by a list of three items, each with a checkmark or an X icon. The first two items have green checkmarks and describe the certificate as being from a trusted authority and having a valid date. The third item has a red X and states that the name on the certificate is invalid or does not match the site's name. At the bottom, the question "Do you want to proceed?" is displayed above three buttons: "Yes", "No", and "View Certificate...".

Security Alert

 outlook.office365.com

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

- ✓ The security certificate is from a trusted certifying authority.
- ✓ The security certificate date is valid.
- ✗ The name on the security certificate is invalid or does not match the name of the site.

Do you want to proceed?

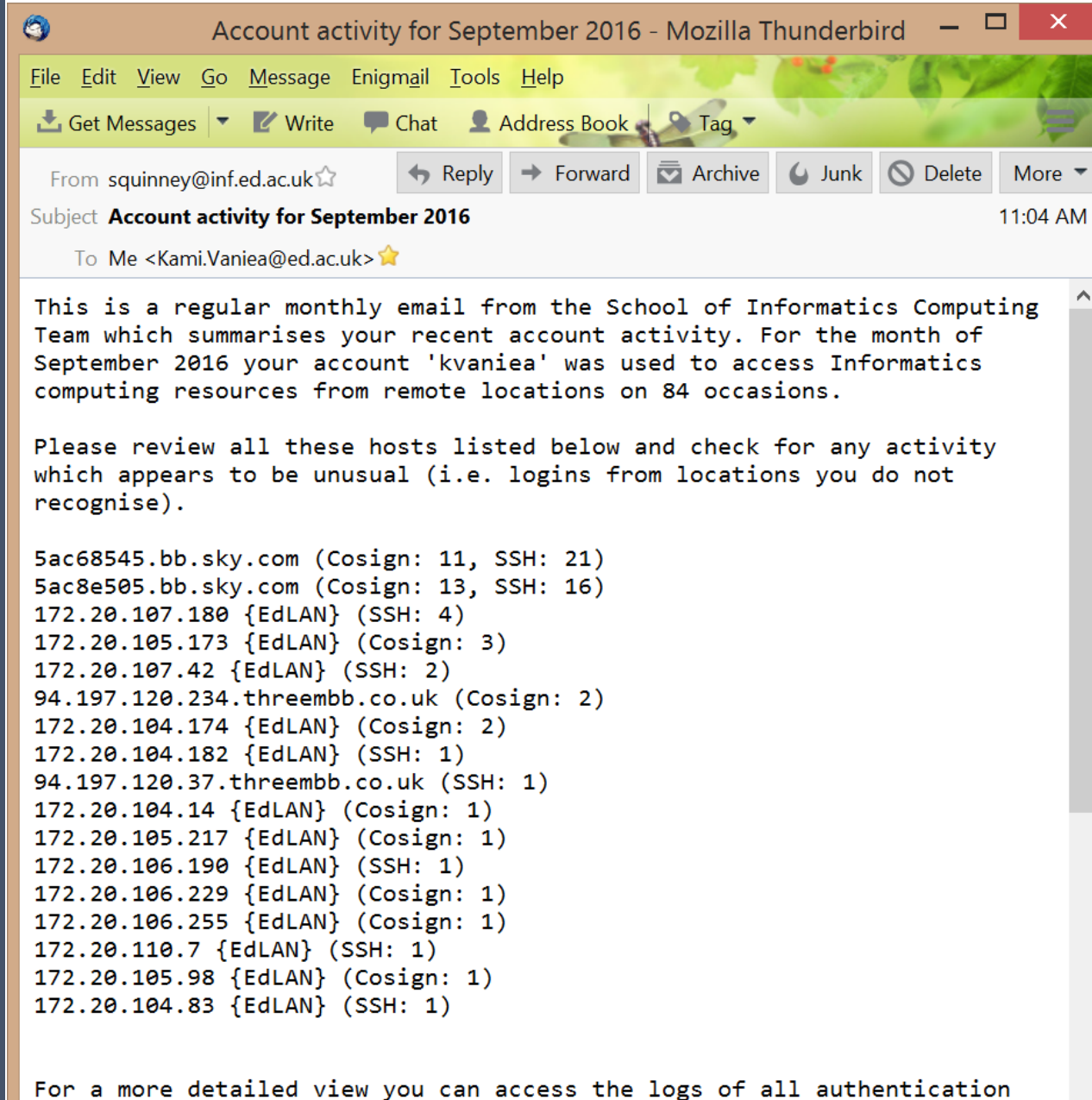
Yes No View Certificate...

Necessary

Explained

Actionable

Tested



Account activity for September 2016 - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Get Messages Write Chat Address Book Tag

From squinney@inf.ed.ac.uk ☆ Reply Forward Archive Junk Delete More

Subject **Account activity for September 2016** 11:04 AM

To Me <Kami.Vaniae@ed.ac.uk> ☆

This is a regular monthly email from the School of Informatics Computing Team which summarises your recent account activity. For the month of September 2016 your account 'kvaniea' was used to access Informatics computing resources from remote locations on 84 occasions.

Please review all these hosts listed below and check for any activity which appears to be unusual (i.e. logins from locations you do not recognise).

5ac68545.bb.sky.com (Cosign: 11, SSH: 21)  
5ac8e505.bb.sky.com (Cosign: 13, SSH: 16)  
172.20.107.180 {EdLAN} (SSH: 4)  
172.20.105.173 {EdLAN} (Cosign: 3)  
172.20.107.42 {EdLAN} (SSH: 2)  
94.197.120.234.threemb.co.uk (Cosign: 2)  
172.20.104.174 {EdLAN} (Cosign: 2)  
172.20.104.182 {EdLAN} (SSH: 1)  
94.197.120.37.threemb.co.uk (SSH: 1)  
172.20.104.14 {EdLAN} (Cosign: 1)  
172.20.105.217 {EdLAN} (Cosign: 1)  
172.20.106.190 {EdLAN} (SSH: 1)  
172.20.106.229 {EdLAN} (Cosign: 1)  
172.20.106.255 {EdLAN} (Cosign: 1)  
172.20.110.7 {EdLAN} (SSH: 1)  
172.20.105.98 {EdLAN} (Cosign: 1)  
172.20.104.83 {EdLAN} (SSH: 1)

For a more detailed view you can access the logs of all authentication

Source

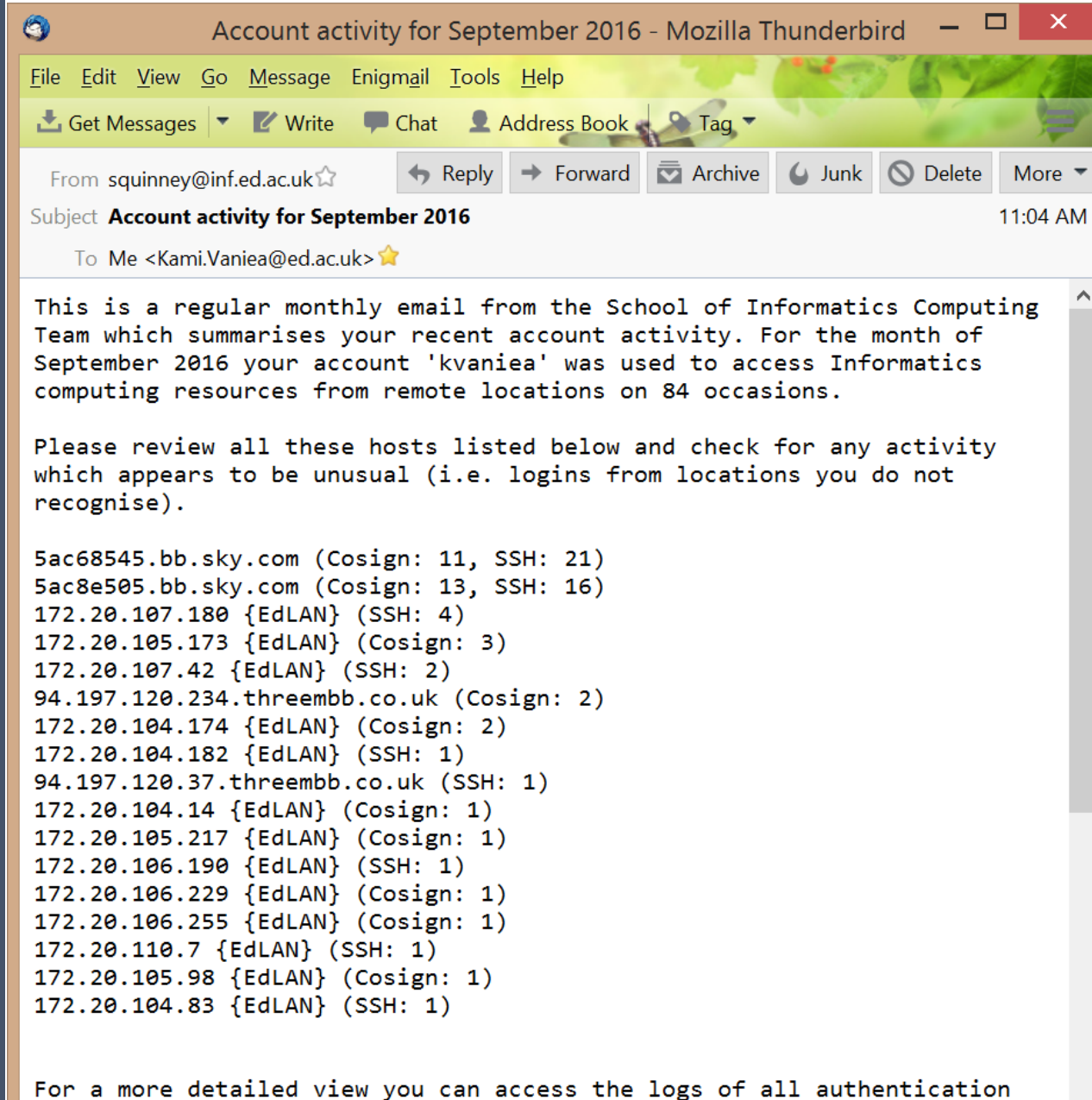
Process

Risk

Unique

Choices

Evidence



Account activity for September 2016 - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Get Messages Write Chat Address Book Tag

From squinney@inf.ed.ac.uk ☆ Reply Forward Archive Junk Delete More

Subject **Account activity for September 2016** 11:04 AM

To Me <Kami.Vaniae@ed.ac.uk> ☆

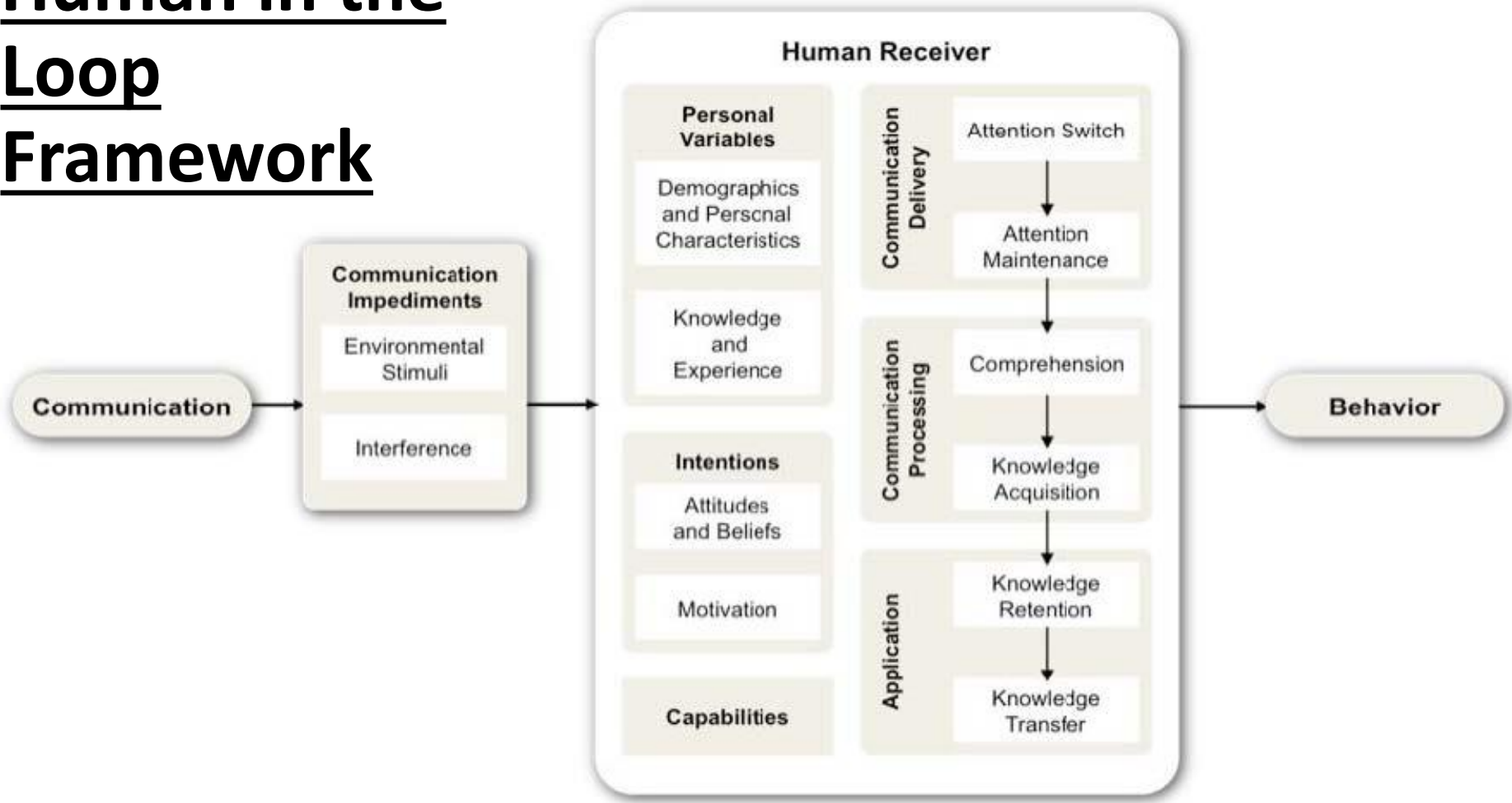
This is a regular monthly email from the School of Informatics Computing Team which summarises your recent account activity. For the month of September 2016 your account 'kvaniea' was used to access Informatics computing resources from remote locations on 84 occasions.

Please review all these hosts listed below and check for any activity which appears to be unusual (i.e. logins from locations you do not recognise).

- 5ac68545.bb.sky.com (Cosign: 11, SSH: 21)
- 5ac8e505.bb.sky.com (Cosign: 13, SSH: 16)
- 172.20.107.180 {EdLAN} (SSH: 4)
- 172.20.105.173 {EdLAN} (Cosign: 3)
- 172.20.107.42 {EdLAN} (SSH: 2)
- 94.197.120.234.threembb.co.uk (Cosign: 2)
- 172.20.104.174 {EdLAN} (Cosign: 2)
- 172.20.104.182 {EdLAN} (SSH: 1)
- 94.197.120.37.threembb.co.uk (SSH: 1)
- 172.20.104.14 {EdLAN} (Cosign: 1)
- 172.20.105.217 {EdLAN} (Cosign: 1)
- 172.20.106.190 {EdLAN} (SSH: 1)
- 172.20.106.229 {EdLAN} (Cosign: 1)
- 172.20.106.255 {EdLAN} (Cosign: 1)
- 172.20.110.7 {EdLAN} (SSH: 1)
- 172.20.105.98 {EdLAN} (Cosign: 1)
- 172.20.104.83 {EdLAN} (SSH: 1)

For a more detailed view you can access the logs of all authentication

# Human in the Loop Framework



Account activity for September 2016 - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Get Messages Write Chat Address Book Tag

From squinney@inf.ed.ac.uk

Subject **Account activity for September 2016** 11:04 AM

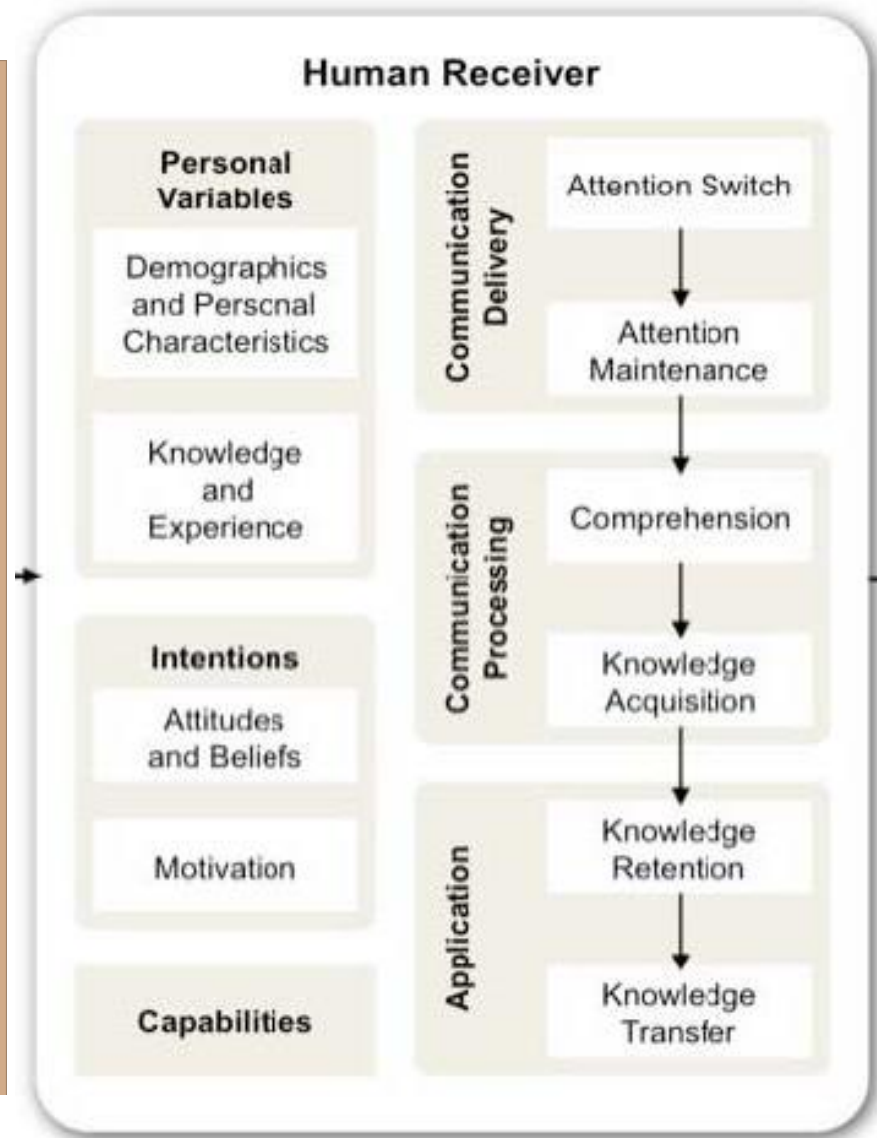
To Me <Kami.Vaniae@ed.ac.uk>

This is a regular monthly email from the School of Informatics Computing Team which summarises your recent account activity. For the month of September 2016 your account 'kvaniea' was used to access Informatics computing resources from remote locations on 84 occasions.

Please review all these hosts listed below and check for any activity which appears to be unusual (i.e. logins from locations you do not recognise).

- 5ac68545.bb.sky.com (Cosign: 11, SSH: 21)
- 5ac8e505.bb.sky.com (Cosign: 13, SSH: 16)
- 172.20.107.180 {EdLAN} (SSH: 4)
- 172.20.105.173 {EdLAN} (Cosign: 3)
- 172.20.107.42 {EdLAN} (SSH: 2)
- 94.197.120.234.threemb.co.uk (Cosign: 2)
- 172.20.104.174 {EdLAN} (Cosign: 2)
- 172.20.104.182 {EdLAN} (SSH: 1)
- 94.197.120.37.threemb.co.uk (SSH: 1)
- 172.20.104.14 {EdLAN} (Cosign: 1)
- 172.20.105.217 {EdLAN} (Cosign: 1)
- 172.20.106.190 {EdLAN} (SSH: 1)
- 172.20.106.229 {EdLAN} (Cosign: 1)
- 172.20.106.255 {EdLAN} (Cosign: 1)
- 172.20.110.7 {EdLAN} (SSH: 1)
- 172.20.105.98 {EdLAN} (Cosign: 1)
- 172.20.104.83 {EdLAN} (SSH: 1)

For a more detailed view you can access the logs of all authentication



# Questions