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?

Yes    No    View Certificate...
I get a version of this email every month telling me about all the places I’ve logged in from.
How could we make these two examples more usable?
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?
Security Alert

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**

---

**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...]
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)
5ac8955.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)
172.20.106.223 {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
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)
5ac8e595.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

Communication

Communication Impediments
- Environmental Stimuli
- Interference

Human Receiver

Personal Variables
- Demographics and Personal Characteristics
- Knowledge and Experience

Communication Delivery
- Attention Switch
- Attention Maintenance

Communication Processing
- Comprehension
- Knowledge Acquisition

Application
- Knowledge Retention
- Knowledge Transfer

Intentions
- Attitudes and Beliefs
- Motivation

Capabilities

Behavior
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
Questions