# Introduction and Landscape

## Computer Security Lecture 1

KAMI VANIEA AND MYRTO ARAPINIS
SCHOOL OF INFORMATICS
19TH SEPTEMBER 2016

# First, the news…

- First 5 minutes we talk about something interesting and recent
- You will not be tested on the news part of lecture
- You may use news as an example on tests
- Why do this?
  1. Some students show up late
  2. Reward students who show up on time
  3. Important to see real world examples

# First, the news…

- Hacked email
  - Colin Powell: http://arstechnica.co.uk/security/2016/09/new-batch-of-leaked-colin-powell-e-mails-lambasts-trump-and-clinton/
  - Hillary Clinton: http://arstechnica.co.uk/information-technology/2016/07/hillary-clinton-e-mail-saga-analysis/

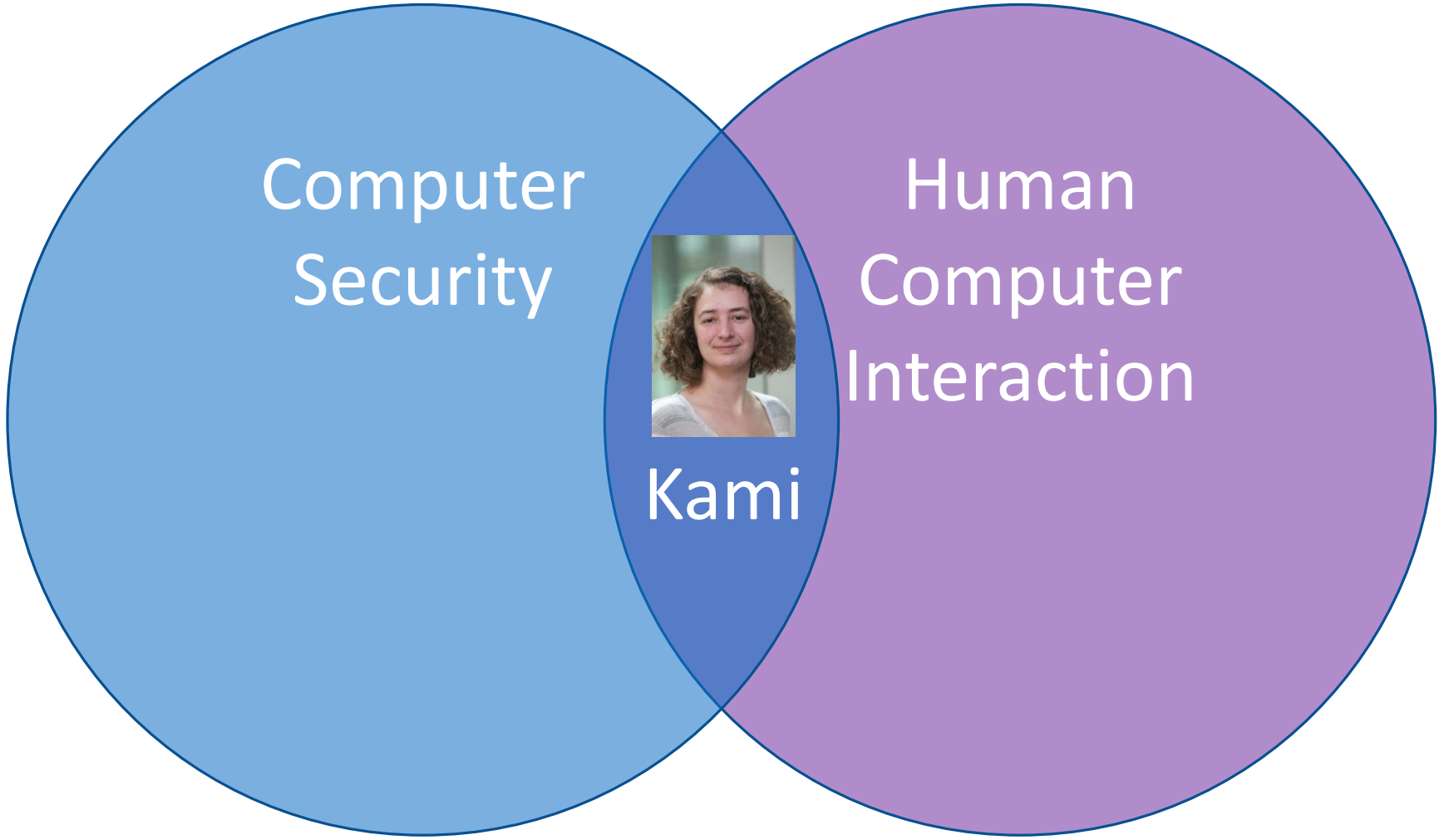
# Kami Vaniea

Pronouncing my last name:

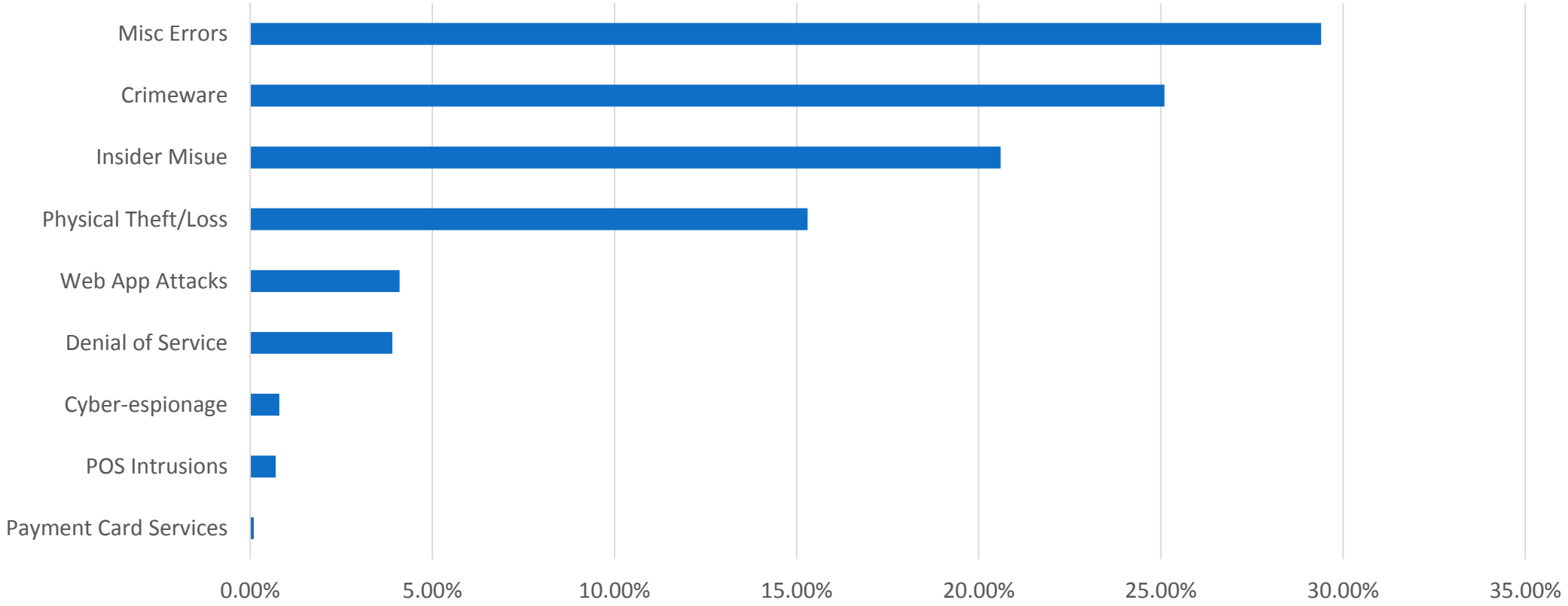
English: Van-yay

French: Vanier

Americans cannot spell French names


Computer
Security
Human
Computer
Interaction
Kami

# People account for 90% of all security incidents



# Today…

- Course introduction
- Common misconceptions
- Basic concepts
- Security properties and their protection

# Which course should I take?

- Computer Security (UG3)
  - Broad survey course
  - Touch on a wide number of security topics
- Secure Programming (UG4)
  - Focuses on how to design secure code
- Cryptography (UG4)
  - Focuses on cryptograph

# What is Computer Security?

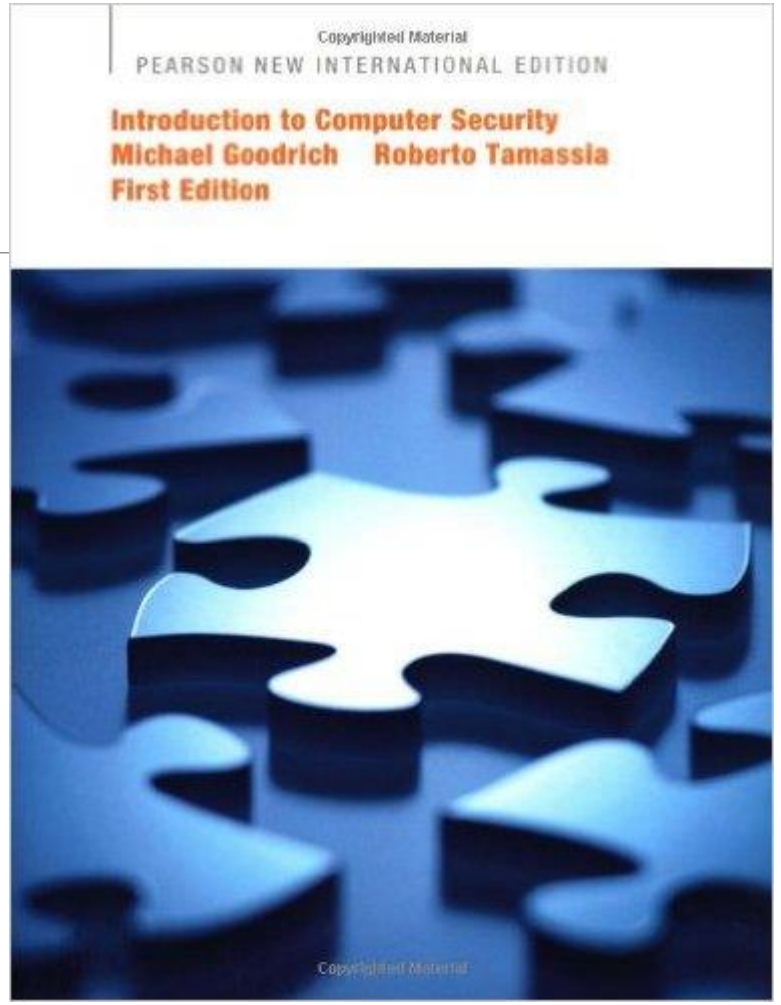
- **Security** is about protecting assets.
- **Computer Security** concerns assets of computer systems: the information and services they provide.
- Just as real world physical security systems vary in their security provision (e.g., a building may be secure against certain kinds of attack, but not all), so computer security systems provide different kinds and amounts of security.
- Computer security is quite vast in scope, touching on many areas besides computer science. In this course we will study the fundamentals , some current internet technologies, and a little bit about engineering and management aspects.

# Lecture plan

- About 30 lectures covering core topics:
  - Risks and threats, Crypto, Protocols, Models, Network, Software, Usability
- Many things not included (despite their relevance):
  - War stories, legalities, security APIs, economics, criminology, Firewall HOWTOs, and Personal advice

# Textbook (not required)

- Recommended (not required) book:
  - **Introduction to Computer Security** by Michael Goodrich and Robert Tamassia Pearson
- Recommended chapters will be posted.



# Standard security course advisory

- Nothing here is intended as an incitement to crack!
- Breaking into systems to “demonstrate” security problems at best causes a headache to overworked sysadmins, and at worst compromises systems for many users and could lead to **prosecution**.
- If you spot a security hole in a running system, **don’t exploit it**, instead consider contacting the relevant administrators confidentially.

# Standard security course advisory

- Security is VERY hard to do correctly all the time.
- Keeping abreast with the latest security patches and methods is difficult; practical security is a matter of weighing up risks, so your advice may not be quickly acted on.
- This is especially true in a relatively low security environment such as a university, where open access has traditionally been put above security, and resources for sysadmin are very tight.

# Responsible security experiments

- **If you want to experiment** with security holes, play wth your own machine, or better, your own private network of machines.
- **One (mostly) harmless way**: use virtualization: e.g., VMWare, VirtualBox, KVT/Xen/UML.
- **If you discover a new security hole** in a standard application or operating system routine that may be running at many sites, then consider contacting the vendor of the software (or vendor of the operating system which contains the software) in the first case. You might also raise the issue in a security forum for discussion, perhaps without providing complete details of the hole.
- The software vendor or other security experts will be able to confirm or deny, and work can begin on fixing the problem.

# In short:

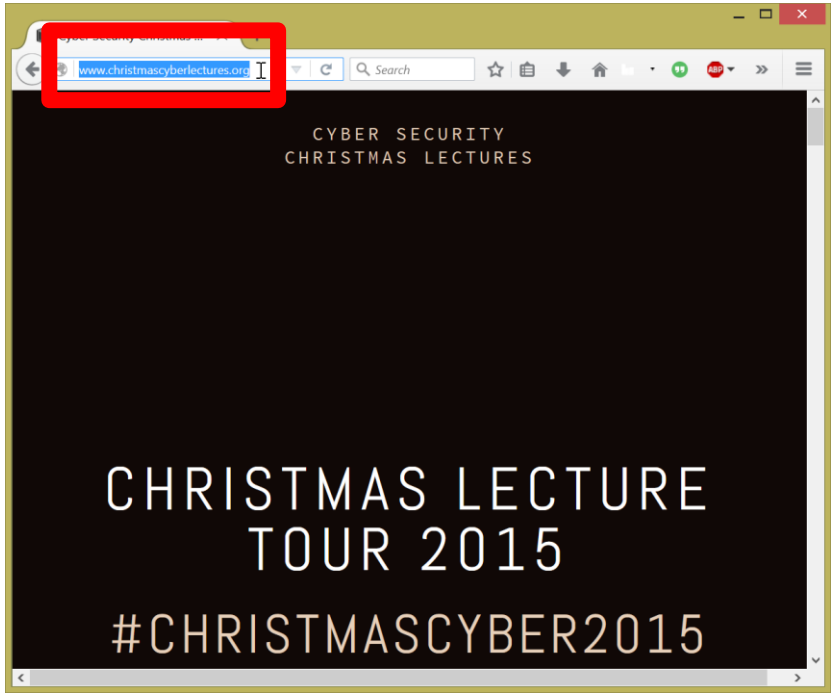
# Please make sure I do not get a visit from Information Services again this year

# Common misconceptions

# Where does this link go to?

**http://facebook.mobile.com**

A. Facebook's main website
B. Facebook's mobile website
C. AT&T's website
D. Mobile's website



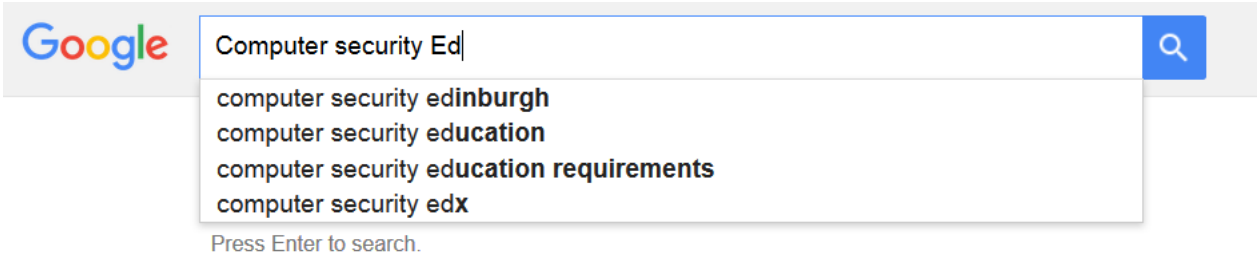
# Like postal addresses, links are read right to left

http://facebook.mobile.com

Edinburgh, IN, USA

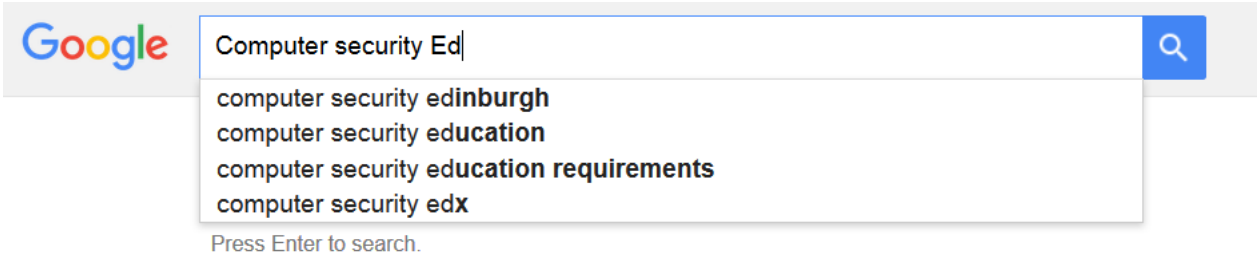

Edinburgh, Scotland

# Does Google know what you have typed before you click enter?




A. Yes
B. No
C. Maybe

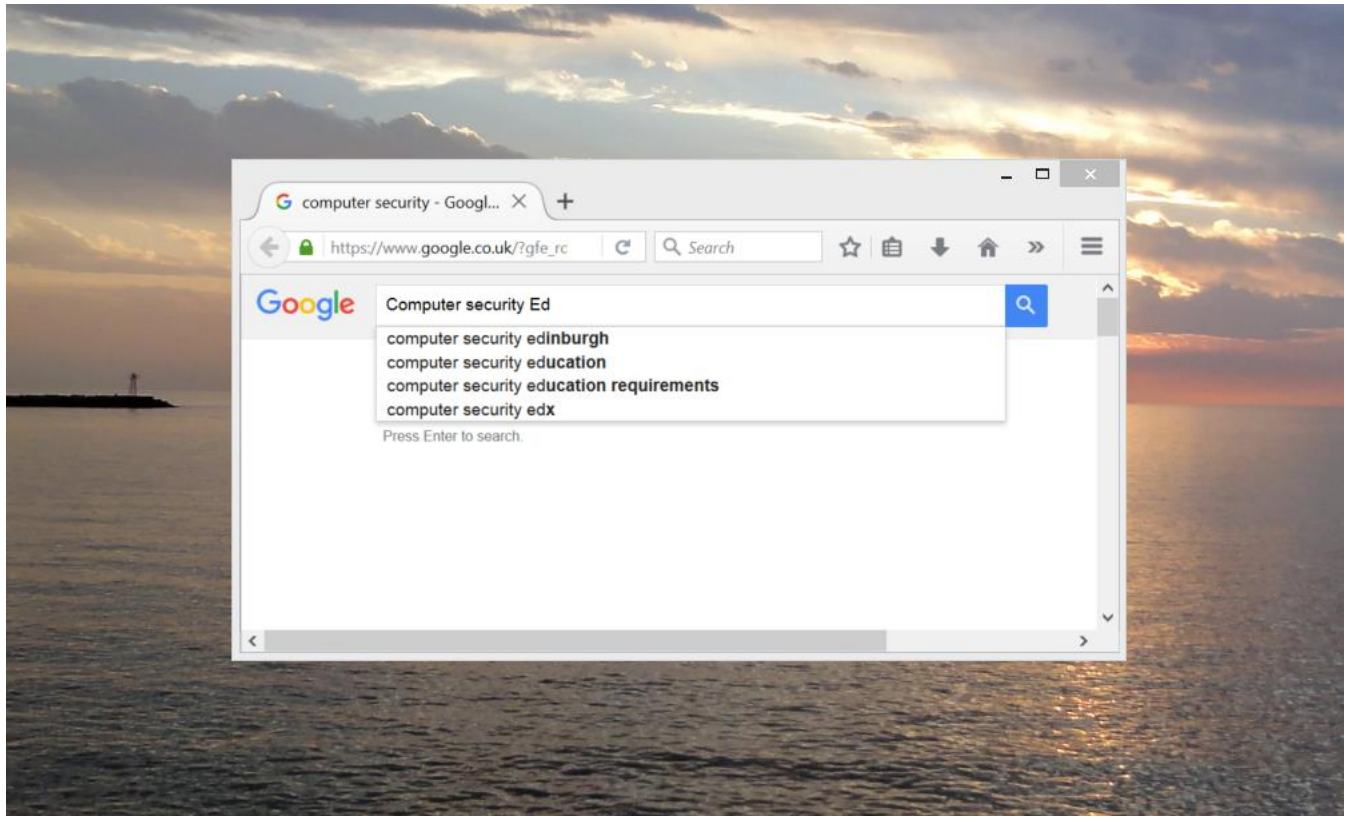
# Does Google know what you have typed before you click enter?




A. **Yes**
B. No
C. Maybe

# Can Google tell what your desktop background is?

A. Yes
B. No
C. Maybe

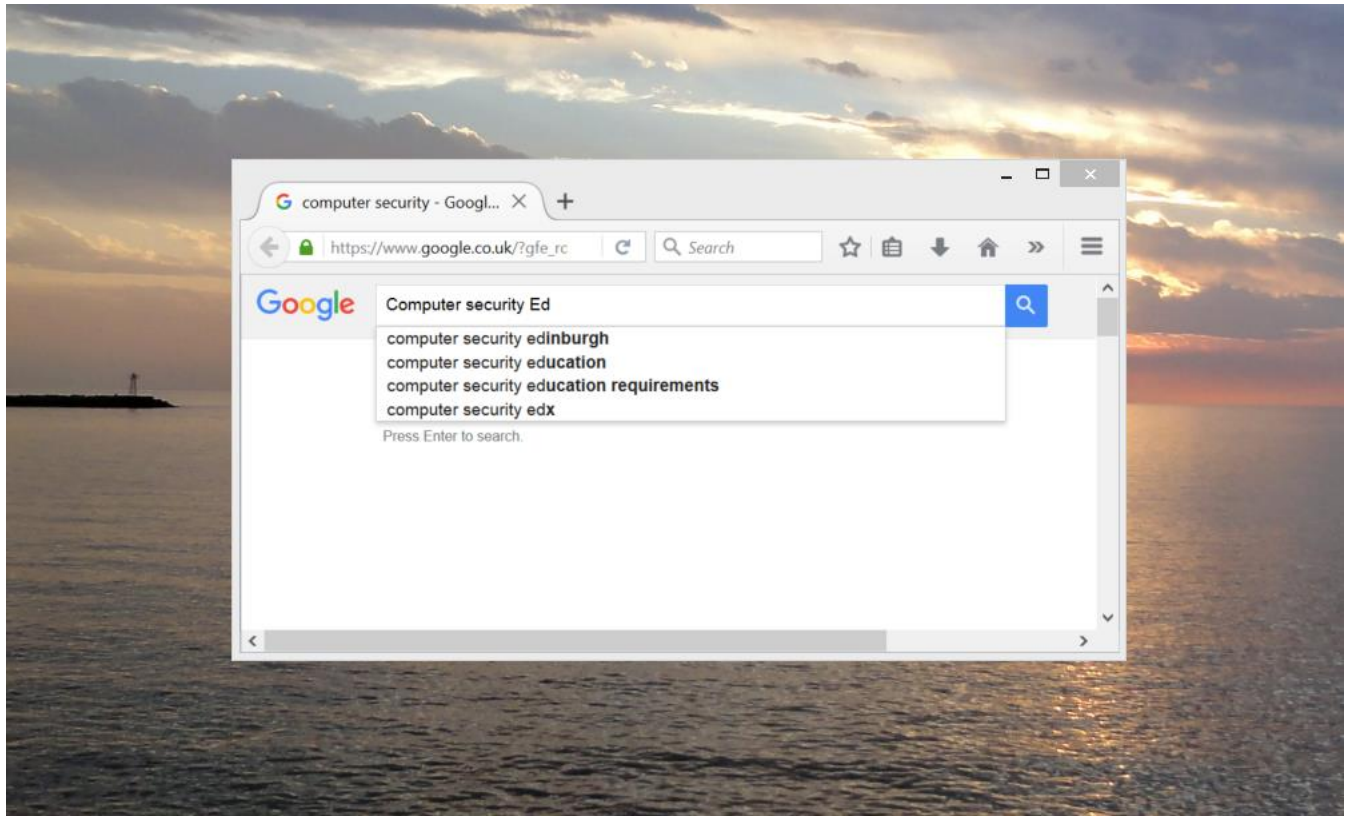


# Can Google tell what your desktop background is?

A. Yes

**B. No**

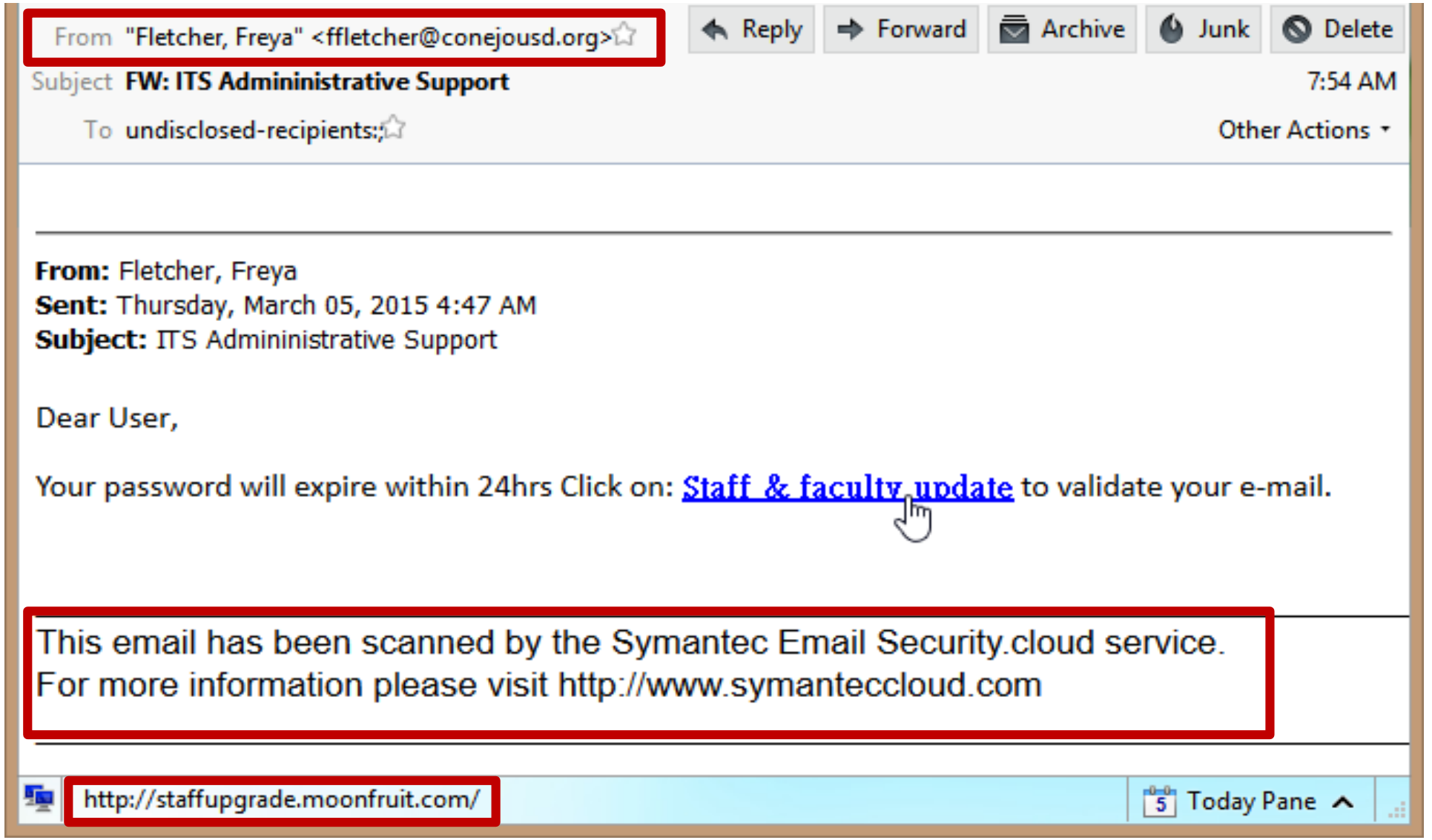
C. Maybe



# Cookies can:

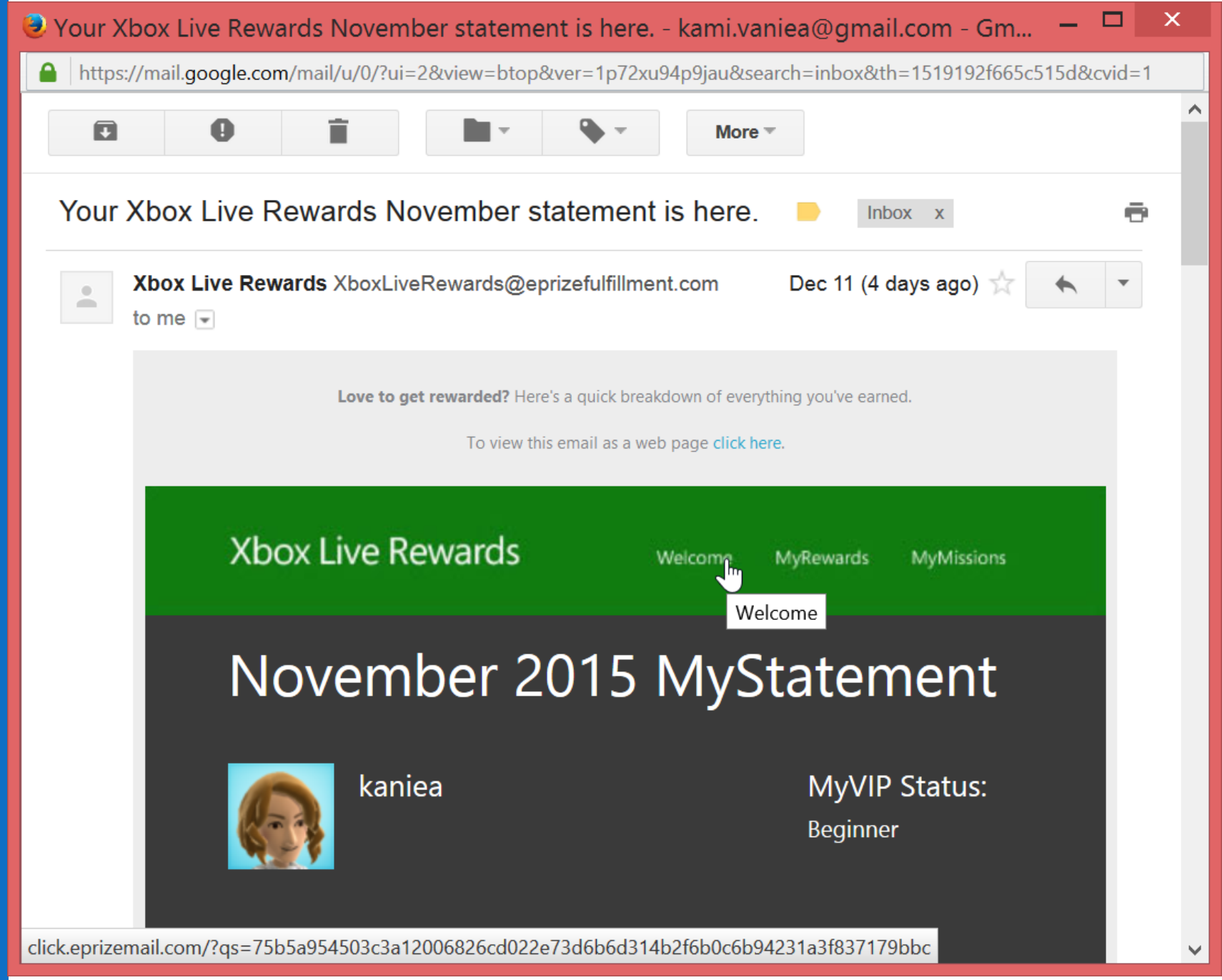
- Be used to track you across web pages.
  - Yes
- Give you malware or viruses.
  - No
- Fill up your computer's hard drive.
  - No
- Contain your passwords in clear text.
  - Yes – but not common
- Be modified by the user.
  - Yes

# What on this email can be trusted?



# Is it safe to click on links in this email?

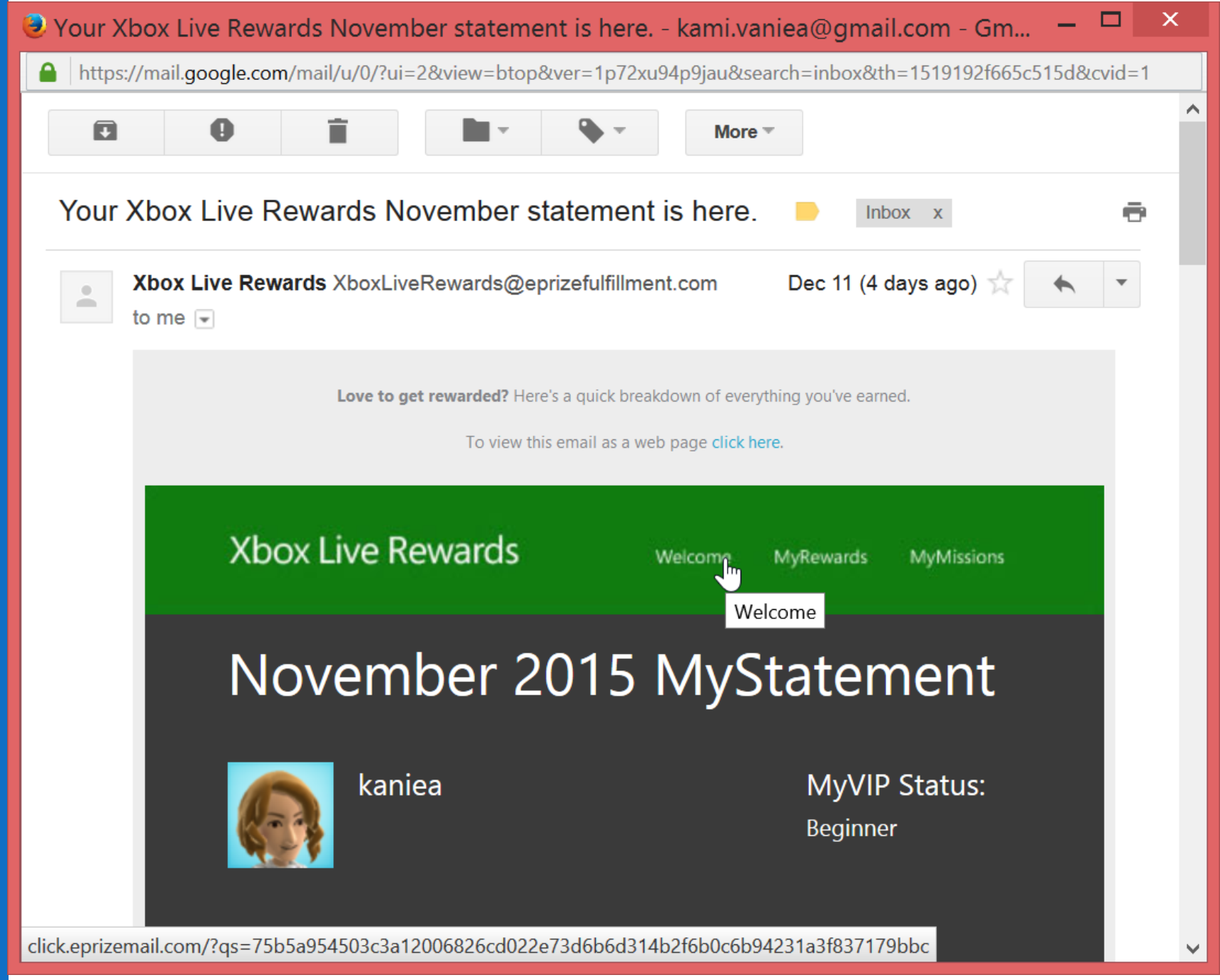
A. Yes
B. No
C. Maybe



# Is it safe to click on links in this email?

A. Yes
B. No
C. Maybe

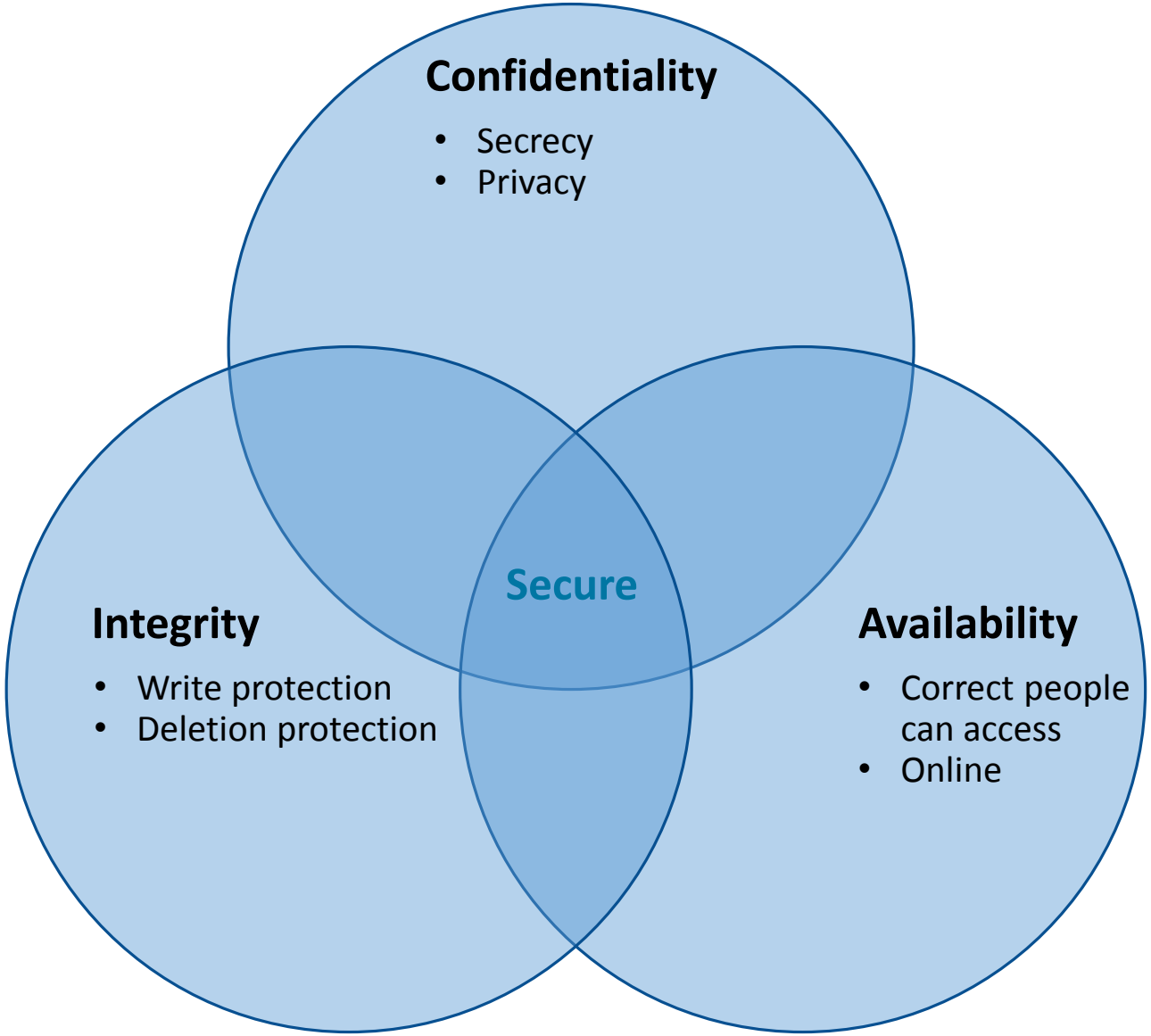
This is actually legitimate email, but there is no way to tell that from just looking at it. The correct answer is that if the email is from Xbox you shouldn't click on something that says "eprizemail".



# Security properties

# Defining Security

- Confidentiality
  - Ensures that computer-related assets are accessed only by authorized parties.
- Integrity
  - Assets can be modified only by authorized parties or only in authorized ways.
- Availability
  - Assets are accessible to authorized parties at appropriate times.



# Security is a whole system issue

- Software
- Hardware
- Physical environment
- Personnel
- Corporate and legal structures

| Security properties to ensure | |
|---|---|
| **Confidentiality** | No improper information gathering |
| **Integrity** | Data has not been (maliciously) altered |
| **Availability** | Data/services can be accessed as desired |
| **Accountability** | Actions are traceable to those responsible |
| **Authentication** | User or data origin accurately identifiable |

# Protection countermeasures

- **Prevention**. Stop security breaches by system design and using security technologies and defenses.
- **Detection**. If an attempted breach occurs, make sure it is detected.
- **Response**. In case of security breach occurs, have a recovery plan. Responses range from restoring from backups or claiming on insurance, through to informing stakeholders and law-enforcement agencies.

# A classic data breach

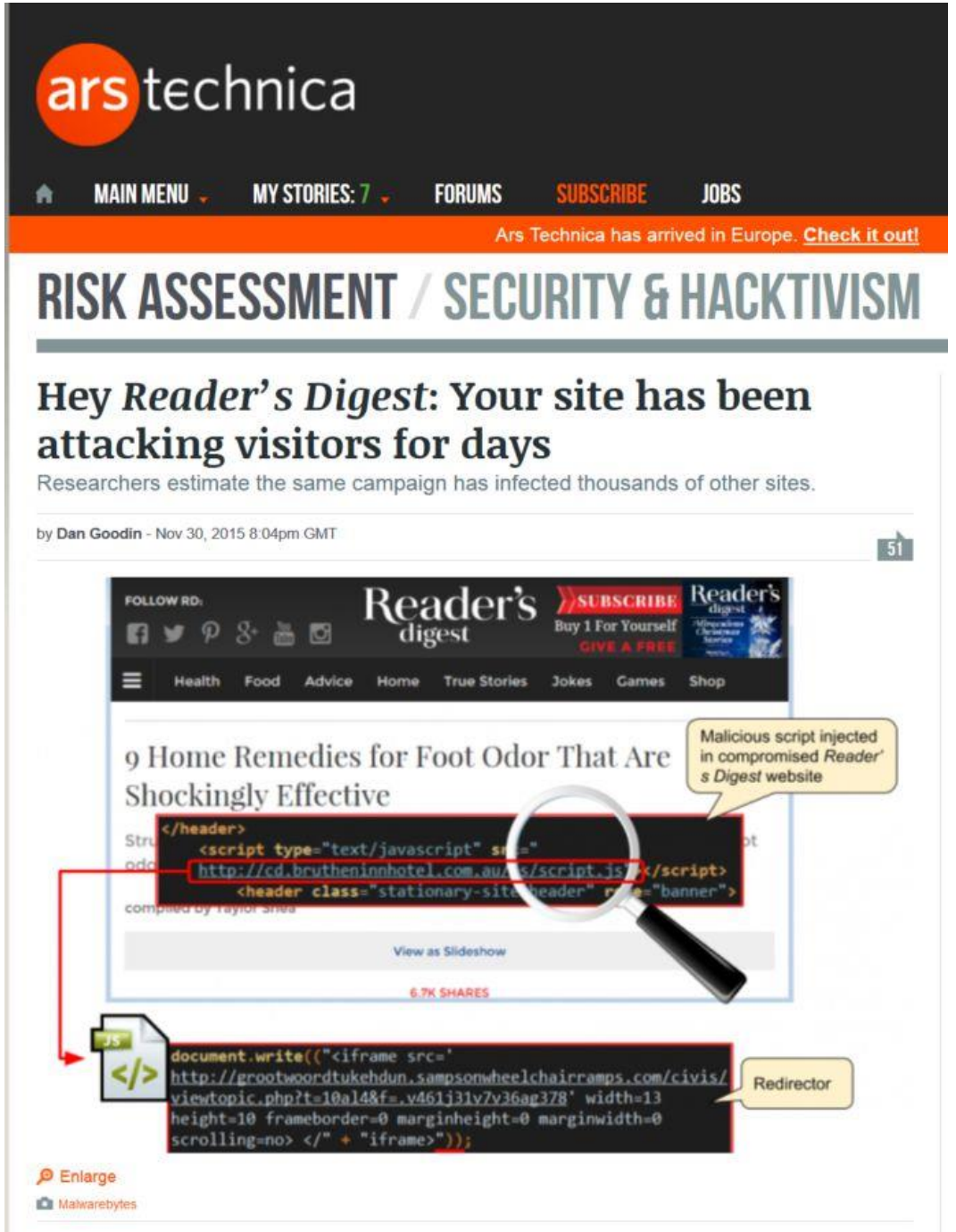
1. Employee is sent a phishing email with a link to a realistic looking internal site.
2. Employee opens the email, clicks the link, and types in her user name and password.
3. Malicious site collects the password and shows the user that everything is actually fine so they are not suspicious.
4. Malicious actor uses user name and password to download sensitive files.

# A classic data breach

1. Employee is sent a phishing email with a link to a realistic looking internal site.
2. Employee opens the email, clicks the link, and types in her user name and password.
3. Malicious site collects the password and shows the user that everything is actually fine so they are not suspicious.
4. Malicious actor uses user name and password to download sensitive files.

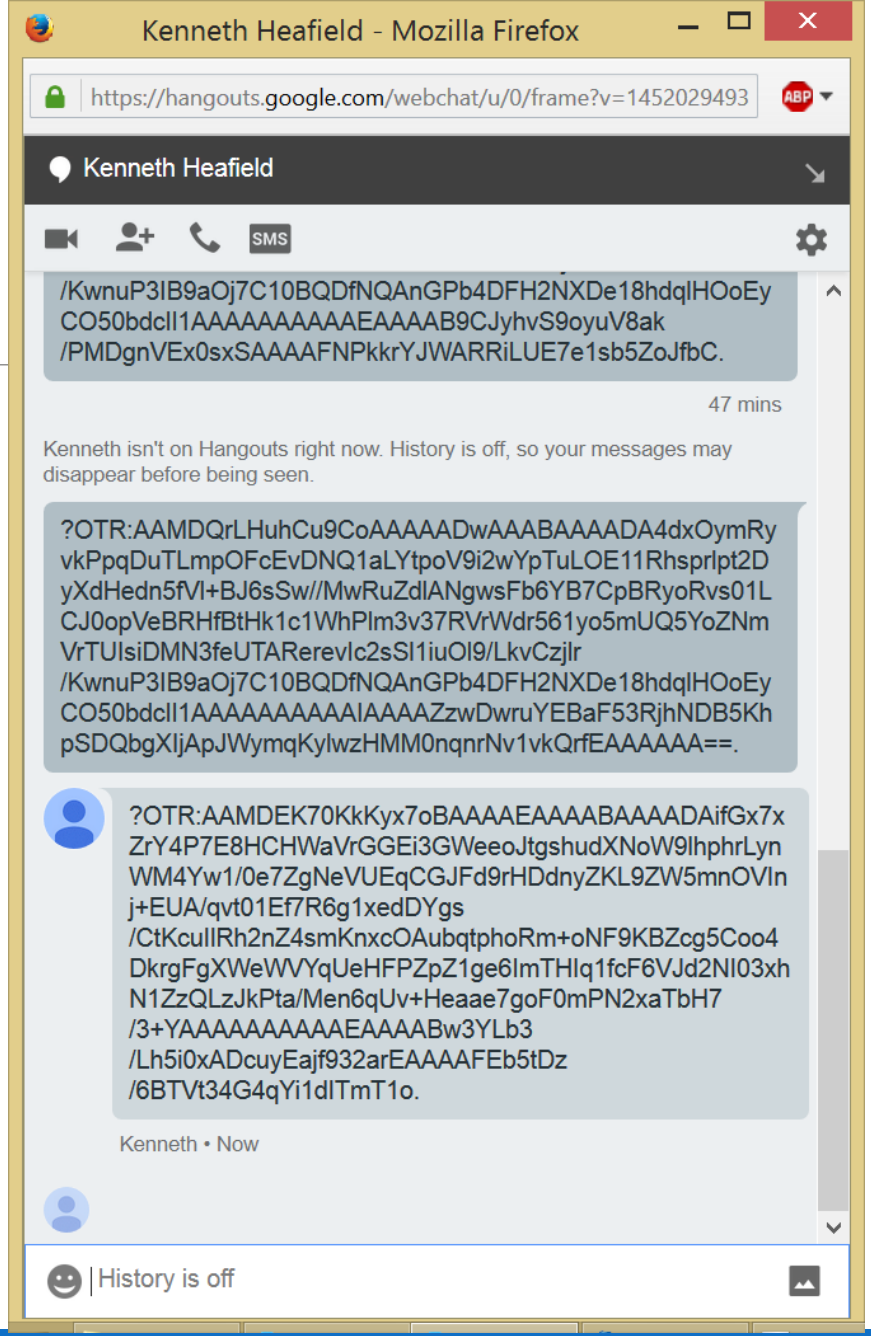
- **Prevention**: detect phishing urls and mark as spam, train employees to notice phishing, identify offsite access of sensitive files and block, encrypt files so useless if leaked.
- **Detection**: Identify that sensitive files have been (past tense) accessed from off site, employee sends email about suspicious email.
- **Response**: Change employee's password, notify CTO, notify insurer, begin post-breach plan.

# Sites are sometimes the last to know they have been compromised



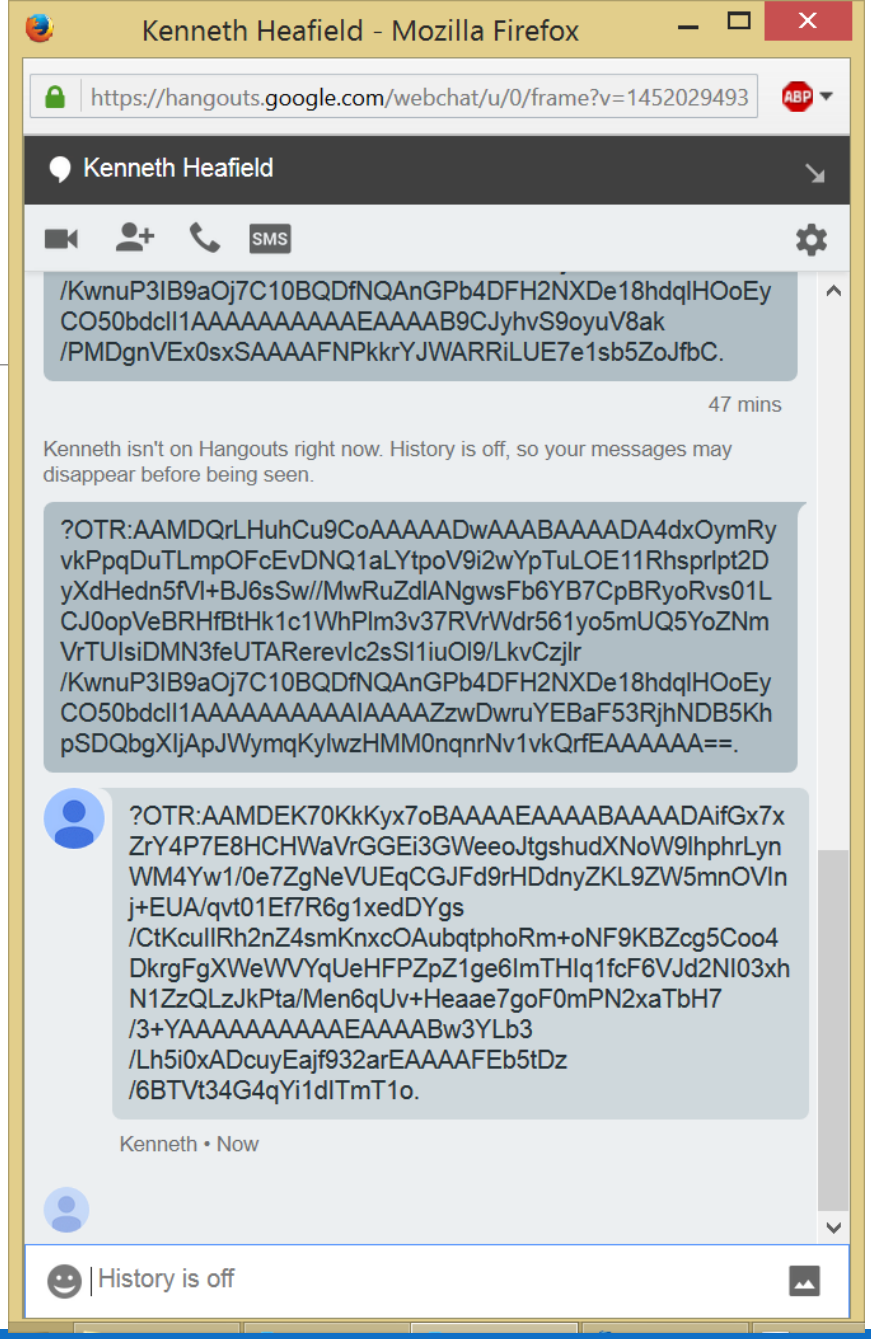
# Confidentiality, privacy, and secrecy

- Confidentiality is characterized as preventing the unauthorized reading of data, when considering access control systems. More generally, it implies unauthorized learning of information.
- The gchat on the right is encrypted. How much can you learn from it anyway?



# Integrity

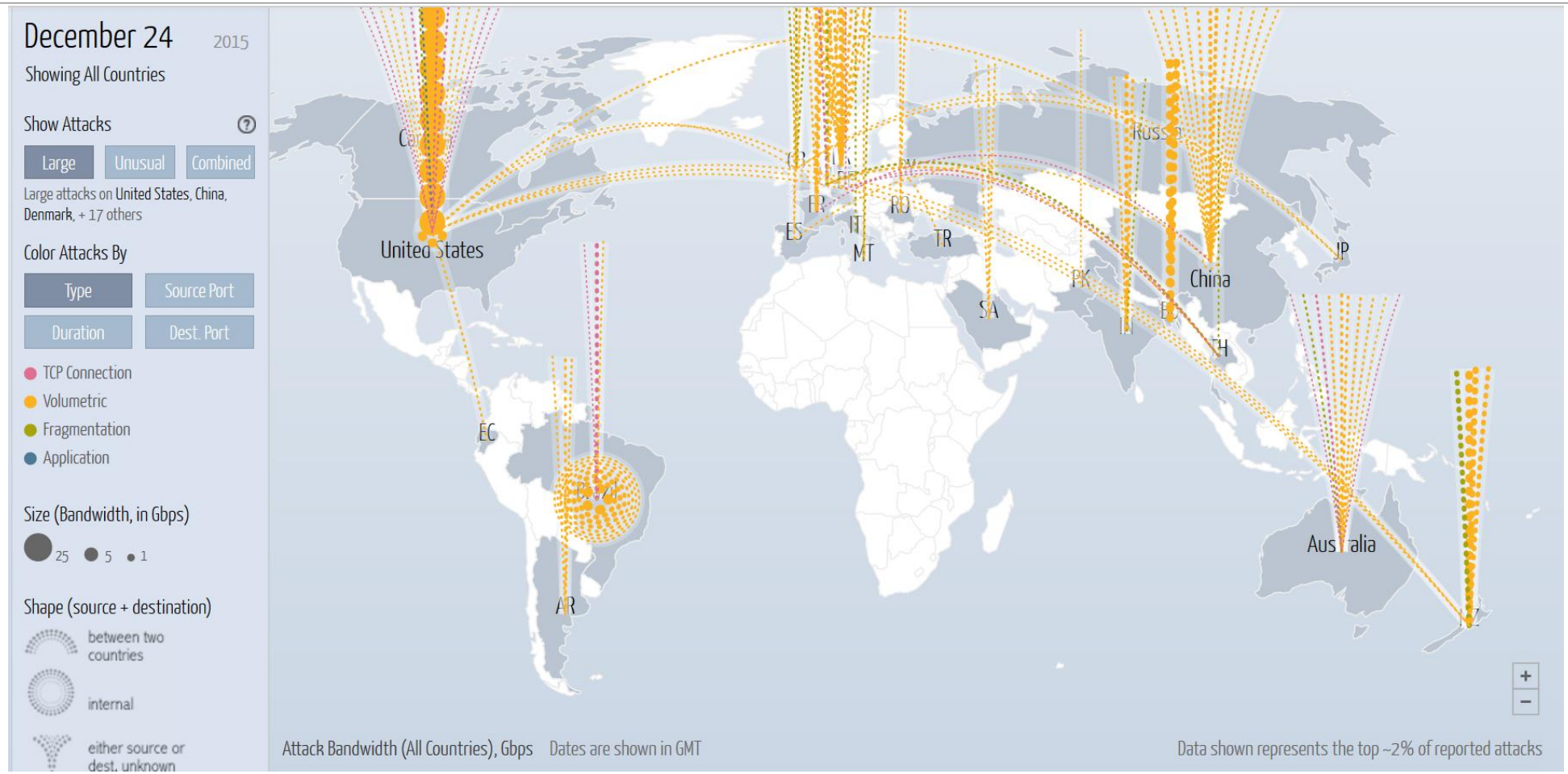
- Data has not been maliciously altered.
- Integrity can have different meanings, in computer security we are primarily concerned with the unauthorized writing of data.
- Examples:
  - Removing a record from a system.
  - An on-line payment system alters an electronic check to read £10000 instead of £100.00



# Availability

- Data or services are accessible as expected.
- Threats to availability cover many kinds of external environmental events (e.g., fire, pulling the server plug) as well as accidental or malicious attacks in software (e.g., infection with a debilitating virus).
- Denial of Service (DOS) threats are the most common form of an Availability threat.

# Availability: DigitalAttackMap



# Accountability

- Actions are recorded and can be traced to the party responsible.
- If prevention methods and access controls fail, we may fall back on detection: keeping a secure audit trail is important so that actions affecting security can be traced back.

# Authentication

- Data or services available only to authorized entities.
- Authentication is necessary for allowing access to some people but denying access to others.
- Authentication typically characterized as:
  - Something you **have** – an entry card, your phone
  - Something you **know** – a password, your mother's maiden name
  - Something you **are** – a signature, fingerprint, way of typing

# Basic concepts

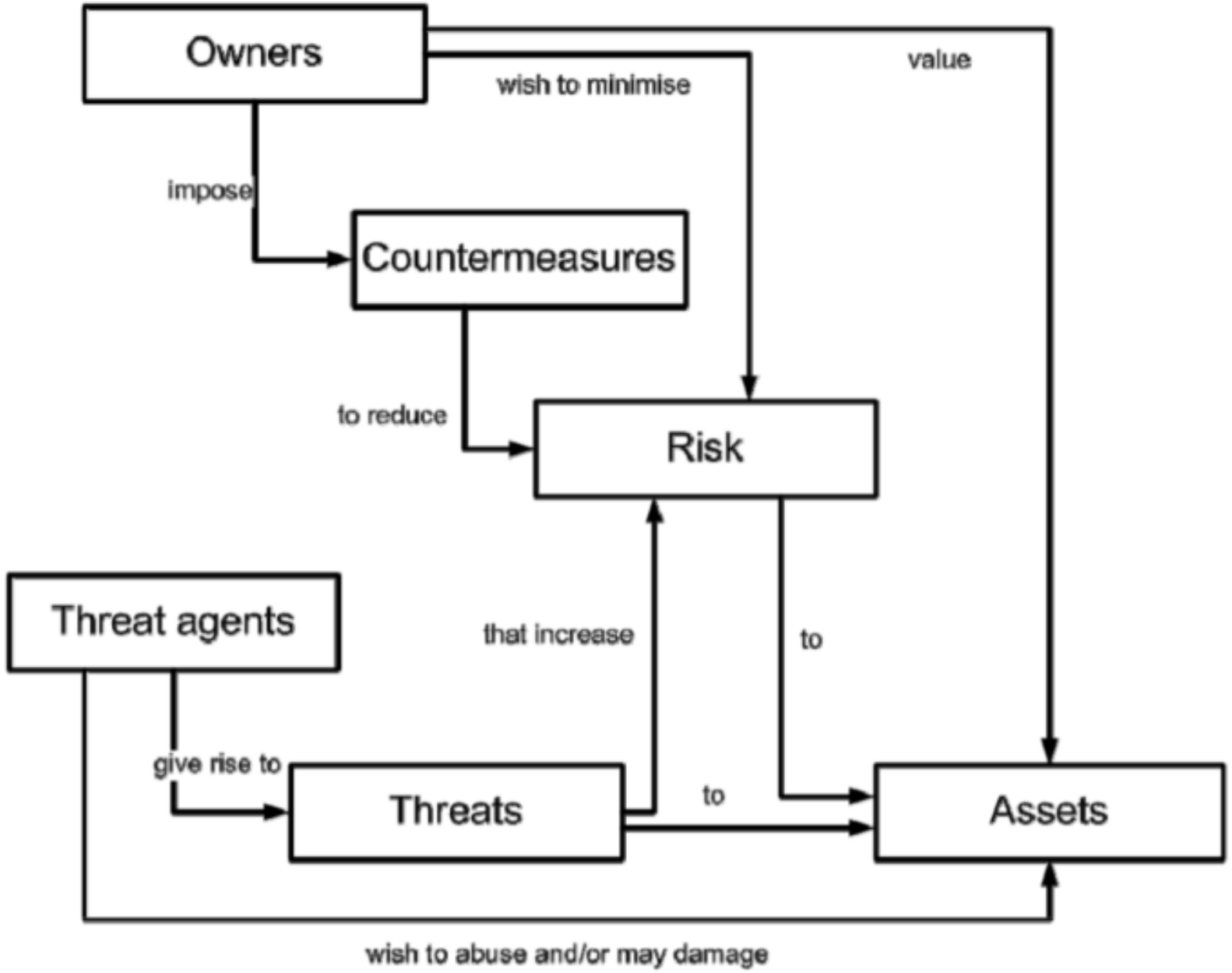
“A system which is unspecified can never be wrong, it can only be surprising.”

# Common Criteria for Information Technology Security Evaluation (CC)

- Security is about protecting assets from threats.
- Threats are the potential for abuse of assets.
- **Owners** value assets and want to protect them.
- **Threat agents** also value assets, and seek to abuse them.
- Owners analyze threats to decide which apply; these risks can be costed.
- This helps select countermeasures, which reduce vulnerabilities.
- Vulnerabilities may remain leaving some residual risk; owners seek to minimize that risk, within other constraints (feasibility, expense).

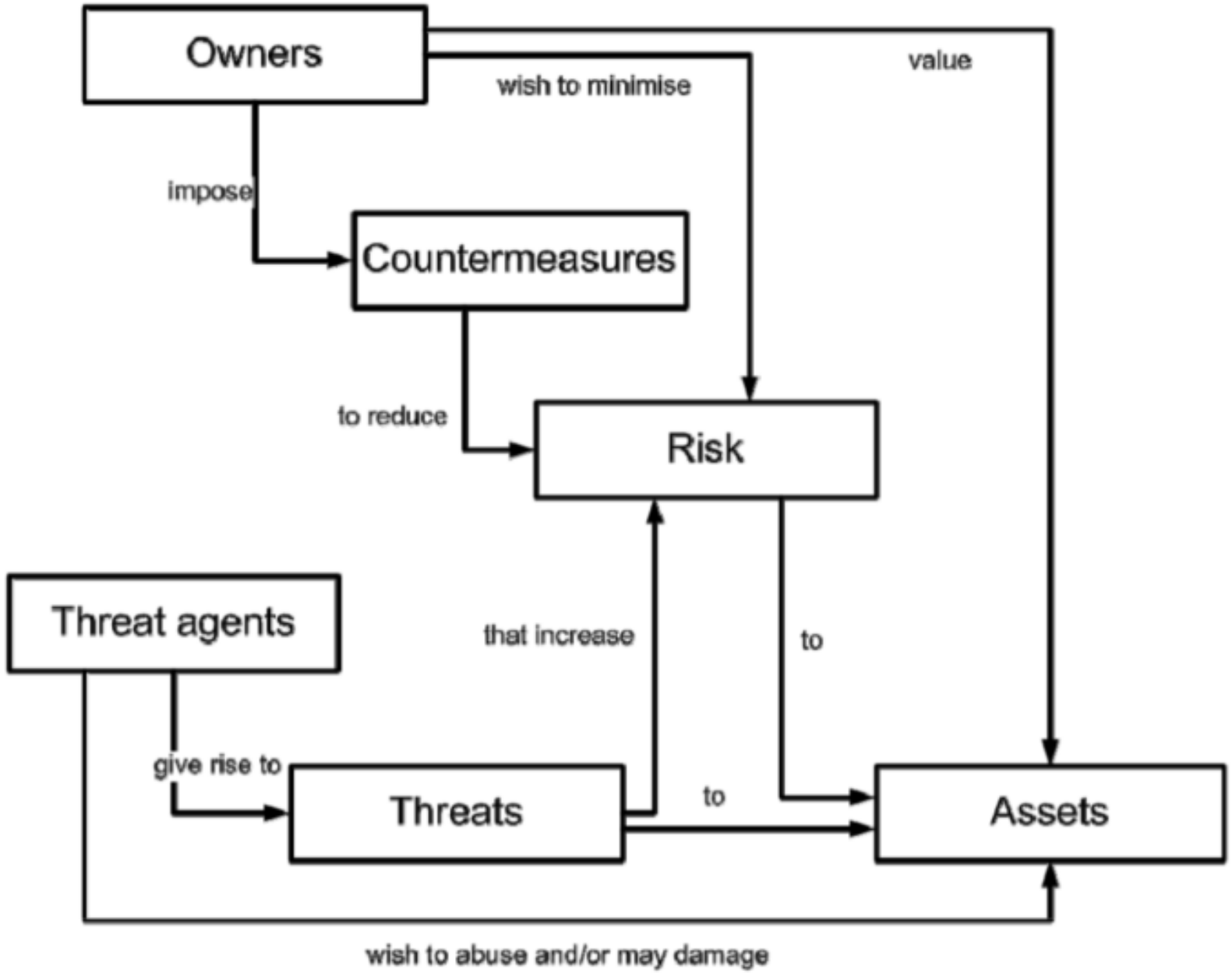
# Security concepts and relationships

-- CC V3.1 R4



# Example: Behavioral Advertising

- **Asset**: User behavior
- **Owner**: The user
- **Threat agent**: Advertisers
- Risks:
  - Malware
  - Tracking
  - Discriminatory pricing



# Questions