

# IT Security and You

UCD IT Services

# What we'll talk about today

- Security, Compliance and Risk.
- Thinking about Security.
- What goes wrong
- Human factors
- Personal Security plan.

# Information

- What is information?
- What kinds of information need to be protected?
- Personal Information examples
  - Student records
  - Staff records
  - Medical records

# Need for Protection

- Reputation.
- Compliance.
  - Data Protection.
  - Acceptable use.
- Maintain reliable services.
- Manage risks.
- Protect vital assets.

## How bad it gets- Sample Reputation damage: Heartland Payment Systems (NYSE:HPY)



Fig: Share price info for Heartland payment systems Jan-Mar 2009.  
Red line indicates date of breach notification.  
Source: NYSE:HPY at finance.google.com

- Previously- 3<sup>rd</sup> largest Payment services company in US.
- Reported 2 year long hack resulting in 113 million credit cards stolen by 20 January 2009.
  - \$12.6 million dollars in direct losses and fines.
  - Class action suit filed.
  - 1 of 3 suspects arrested Jun 2009.
- But also:
  - By 1<sup>st</sup> March company share price had fallen from 1<sup>st</sup> January price of \$18 to \$4.
  - By March 2010, price had not fully recovered.

# Background

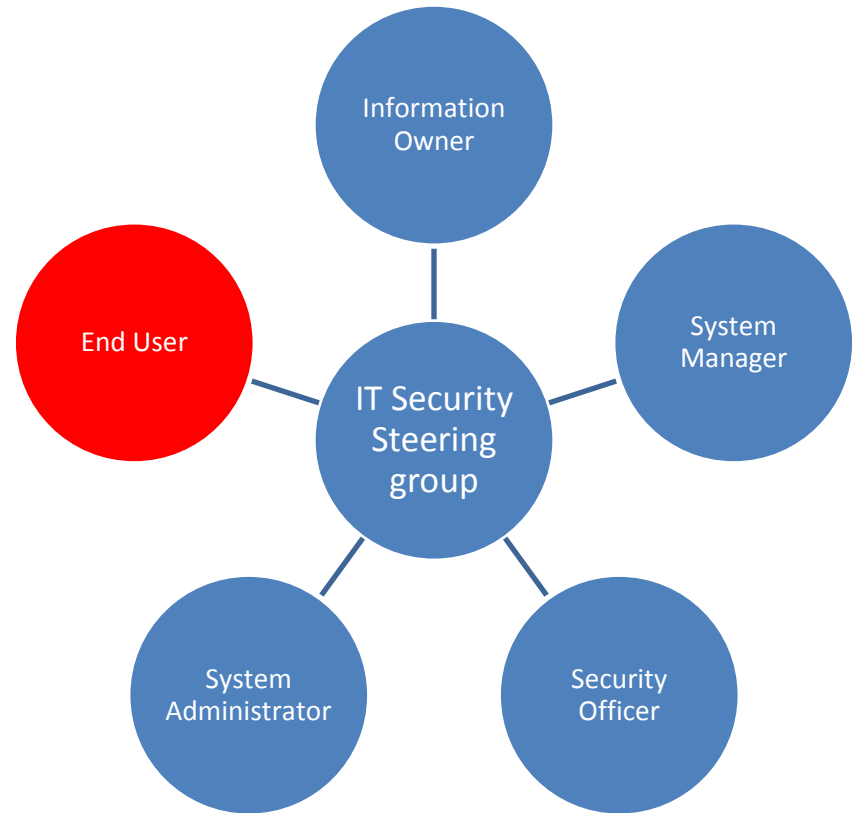
- What is UCD's Security Policy?
- UCD Acceptable Use policy and EICT
- Administrative IT Security Policy
- Approved by UCD senior management
  - AUP by Governing Body
  - IT Admin Steering group.
  - IT Security steering group propose policy at UCD.

# What does it say?

- Allocates ownership of data and management of Security by role.
  - Information Owner.
  - Information Manager.
  - Information User.
- Level of security applied is determined by classification of material.
- Everyone has a role.

# Who looks after security

- Defined roles
- IT Security Steering group
- Information Owner
- System Manager
- Security Officer
- System Administrator
- End User





# IS Management at UCD- Security Principles

- UCD generates, manages and is entrusted with private, confidential and sensitive information.
- The University is committed to protecting the confidentiality of all our information, ensuring that information is
  - accurate,
  - complete
  - available for appropriate uses.

# Data Protection at UCD

# Data protection

1. Obtain and process *fairly*
  2. Keep for one or more specified and lawful purposes\*
  3. Process only in ways compatible with these purposes
  4. Keep safe and secure
  5. Keep accurate and up-to-date
- \* *Does not apply to personal data kept for statistical, research, or other scientific purposes if used in a way that will not harm or cause distress to the Data Subject*

# Data Protection Principles

- Obtain and process information fairly
- Keep it only for one or more specified, explicit and lawful purposes
- Use and disclosure only in ways compatible with these purposes
- Keep it safe and secure
- Keep it accurate, complete and up-to-date
- Ensure it is adequate, relevant and not excessive
- Retain for no longer than is necessary
- Give a copy of his/ her personal data to that individual, on request

# Overview of Data Protection Policy and Legislation.

- Right to the protection of privacy with regard to the *processing of personal data*.
- *Processing*: obtaining, recording or keeping, collecting, organising, storing, altering or adapting, retrieving, consulting or using, disclosing, blocking, erasing or destroying
- *Personal data*: data relating to a living individual who can be identified
  - either from the data or
  - from the data in conjunction with other information in the possession of the data controller

# Overview of DP – rights s.1

- “Sensitive personal data” means data relating to:
  - racial or ethnic origin, political opinions or religious or philosophical beliefs
  - trade union membership
  - physical or mental health or condition or sexual life
  - the commission or alleged commission of any offence, or
  - any proceedings for an offence committed or alleged to have been committed

## Overview of DP – rights s.3,4,6

- Right to be informed if data are kept, to include:
  - a description of the data
  - the purposes for which they are kept (s.3)
- Right of access to the data (s.4)
  - 40 day statutory time limit
- Right of correction, blocking or erasure if data are incorrect (s.6)

## Overview of DP – 8 rules s.2

1. Obtain and process *fairly* (see next slide)
2. Keep for one or more specified and lawful purposes\*
3. Process only in ways compatible with these purposes
4. Keep safe and secure
5. Keep accurate and up-to-date

\* *Does not apply to personal data kept for statistical, research, or other scientific purposes if used in a way that will not harm or cause distress to the Data Subject*



## Overview of DP – rules s.2

- Personal data are deemed to be processed fairly *only if* the Data Subject is informed of:
  - Identity of Data Controller
  - Purpose of processing the data
  - Any disclosures of data
  - Questions to which answers are optional
  - The right of access and to rectification
  - Any obtaining not directly from the subject

## Overview of DP – rules section 2

- Ensure it is adequate, relevant and not excessive
- Retain for no longer than is necessary for the specified purpose or purposes\*
- Provide a copy of his/her personal data to any individual on request

**Does not apply to personal data kept for**

- ***Statistical, research, or other scientific purposes***

***But only if used in a way that will not harm or cause distress to the Data Subject.***

## **Data Protection- Important Don'ts:**

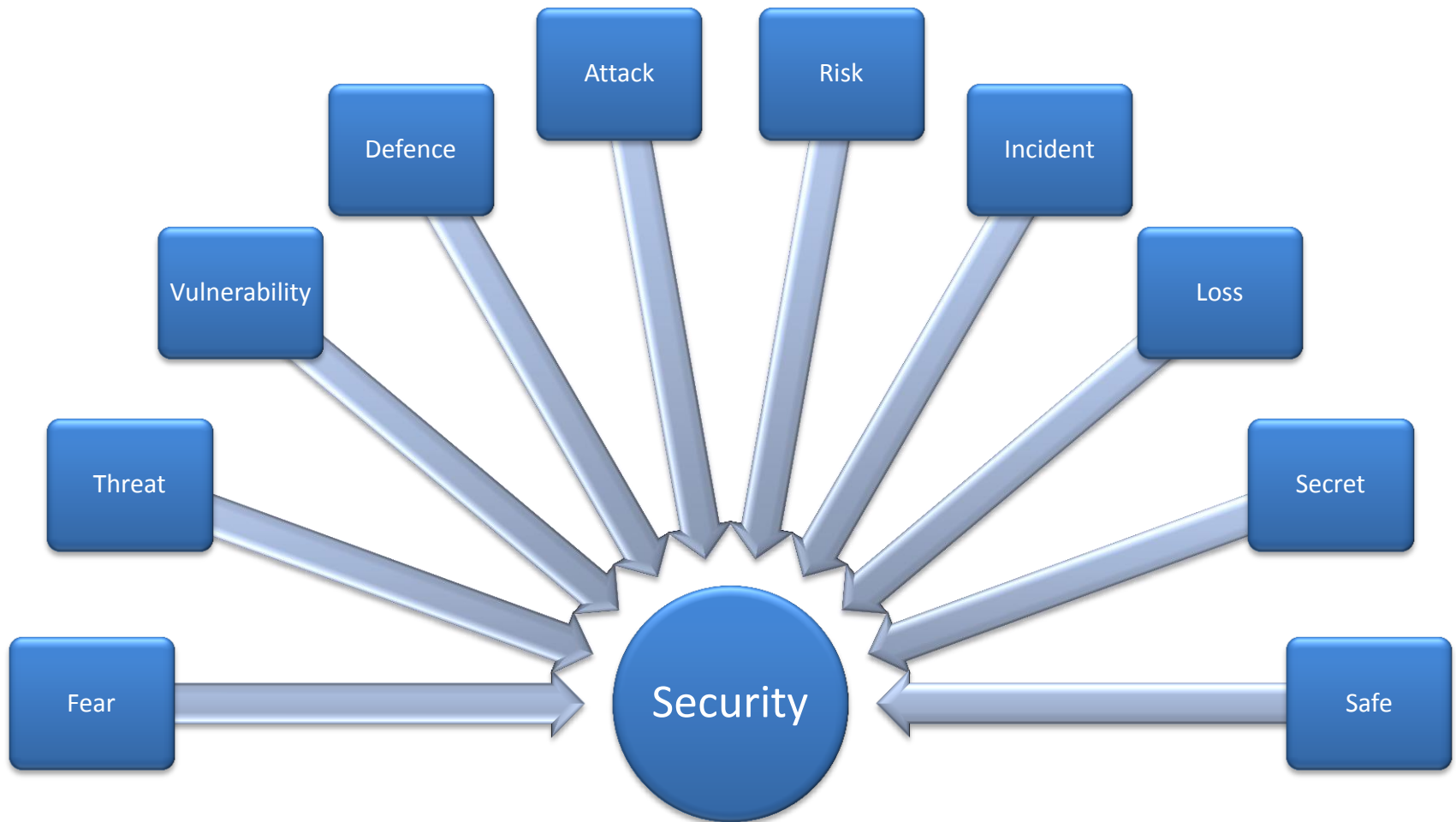
- Don't disclose data to third parties without consent
- Don't retain personal data any longer than necessary (Think about required uses)
- Don't collect personal data that are irrelevant or excessive for the purpose for which they are being collected

## Data Protection-Common issues

- **Ensure review and audit procedures are in place to ensure data are accurate, complete and up-to-date.**
- **Only disclose personal data to work colleagues where there is a legitimate administrative reason.**
- **Only those who need to know the health condition of an individual should have access.**
- **Never identify a student when posting personal data about exams.**

What is Security?

# What does Security mean?



# Security and Risk

- Risk is a possible future event.
  - It can be quantified (how likely, size of event) based on previous experience and data.
  - It can be positive (e.g. Investment for gain).
  - Mostly seen as negative (loss incidents).
- But you can always have an unexpected incident.

# Information Security

- Concerned with Negative risk in Information.
- Basic premise is to identify and manage Risk.
  - Prior experience= known risk.
  - Prior events= known costs.
  - But.. The future is not the past.
- Think about what happens to others.
  - Plan, implement, check and act.



# Risk management

Event	Likelihood Low-High	Impact Low-High	Risk rating (Low-Crit)	Mitigation	Residual risk (low-high)
e.g. Laptop Disk failure	High	High	Crit	Back up data	Low
Plane crash into data centre	Low	High	Med	Offsite data Backup	Low

# UCD data classification

Reason for Classification	Strictly Confidential	Confidential	Controlled
<b>Legal Requirement</b>	Protection of information is required by law or regulatory instrument. Information is subject to strictly limited distribution within and outside the University.	UCD has a legal, regulatory or contractual obligation to protect the information.	Protection of information is at the discretion of the owner or custodian
<b>Reputation Protection</b>	Disclosure would cause exceptional or long term damage to the reputation of the University, or risk to those whose information is disclosed.	Could cause harm to the reputation of the University	Low risk of embarrassment or reputational harm
<b>Commercially sensitive</b>	May have serious or long term negative financial impact on the University	May have short term financial impact on the university	
<b>Other Risks</b>	Information which provides access to resources, physical or virtual	Smaller subsets of protected information from a school or department	General university information
<b>Public/ Unrestricted</b>	Not sensitive		

# UCD Control policy

<b>Physical access</b>	<p>Stored in a locked cabinet at all times when unattended.</p> <p>Central Server Systems storing information must be housed in a secure datacentre environment.</p> <p>Documents should not be stored on a PC or laptop unless encrypted.</p>
<b>Copies and distribution</b>	<p>Must only be available to named UCD Staff and sections on the distribution list.</p> <p>Copies may only be made available to other individuals with the written permission of the document owner.</p> <p>Information may only be printed or photocopied in the presence of an authorised user.</p>

<b>Physical Transfer (paper documents)</b>	Paper documents must be transferred in a sealed container / envelope. If posted, these must use registered post.
<b>Electronic storage</b>	<p>Must be stored in systems accessible only to specified users authorised by the data owner.</p> <p>Suitable encryption must be used to protect information in electronic format, such as on a mobile device.</p>
<b>Electronic transfer (e-mail, FTP etc)</b>	Must be encrypted if transferred via a network.
<b>Destruction of physical media</b>	<p>All Strictly Confidential information must <u>brought</u> directly to a shredding facility for cross-cut shredding &amp; disposal.</p> <p>Storage media (including laptop disks) which have ever handled Strictly Confidential information must be disposed of according to procedures defined by the System Manager.</p>
<b>Marking</b>	Items corresponding to this classification which are generated within UCD must carry the Must carry a marking "Strictly Confidential- Circulation Limited to Authorised Users", and have a distribution list which is visible on printed and electronic copies of information.
<b>System controls</b>	<p>Information may only be processed on approved UCD systems conforming to the security requirements of the Information Security Officer, and implemented by a System Manager.</p> <p>Systems and applications providing access to confidential information must have appropriate login banners. Access is authorised only to named individuals that have received appropriate training.</p>

So, What do I do?

# Security is Routine!

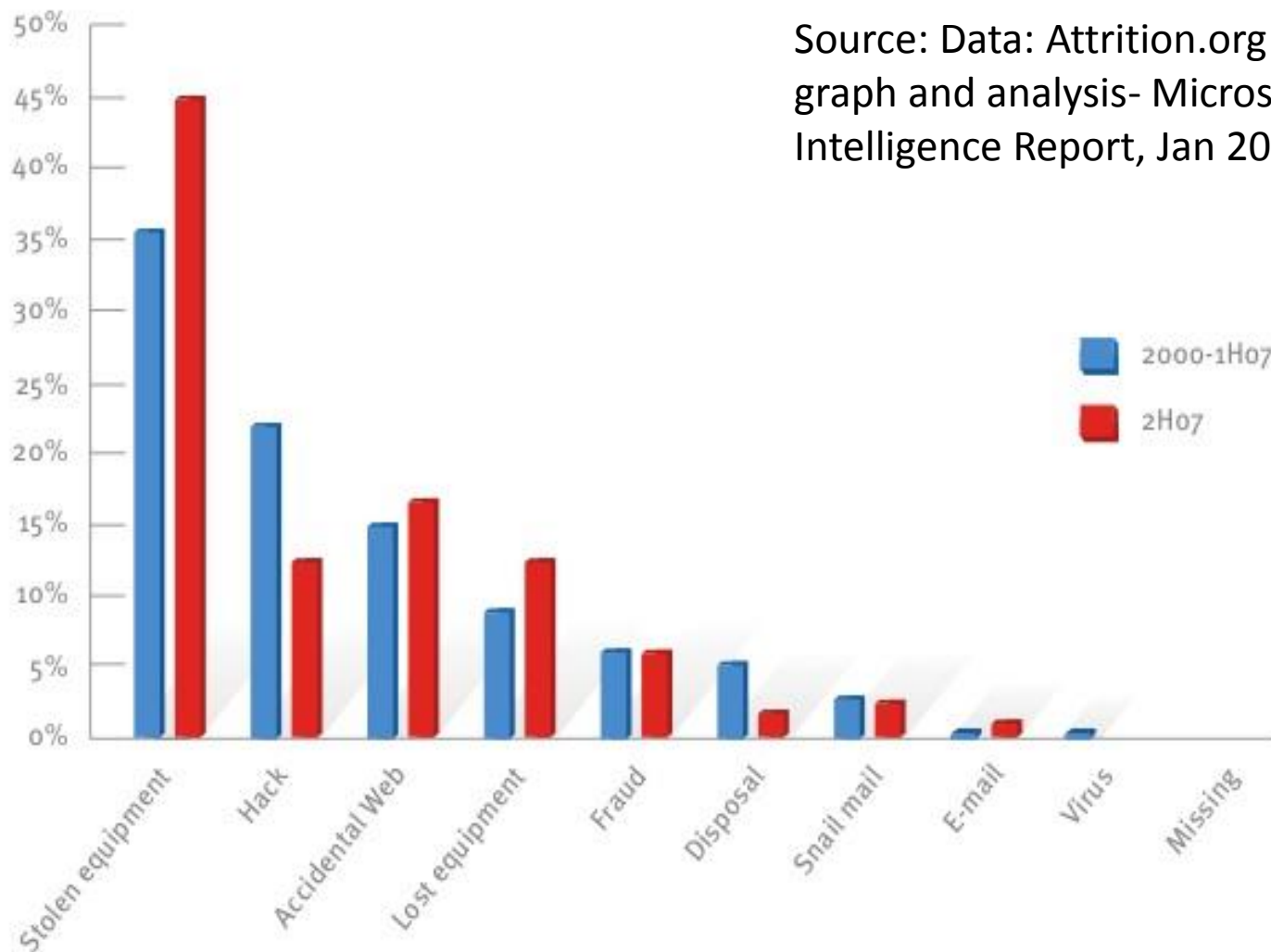
- Things I do every day
- Things I do weekly
- Things I do quarterly
- Things I do when the situation arises-
  - New Computer
  - Recycle computer
  - Something bad happens

# Most important

- Regular tasks
  - Get your computer set up correctly.
  - Get regular updates.
  - Set and protect strong passwords. Change them regularly.
  - Use email and the internet securely.
  - Back up your data.
  - Lock your screen every time you leave your computer.
- Ask for help when you need it!

# What used to happen

FIGURE 2. Security breach incidents by type, 2000–1H07, and 2H07 alone, expressed as percentages of the total





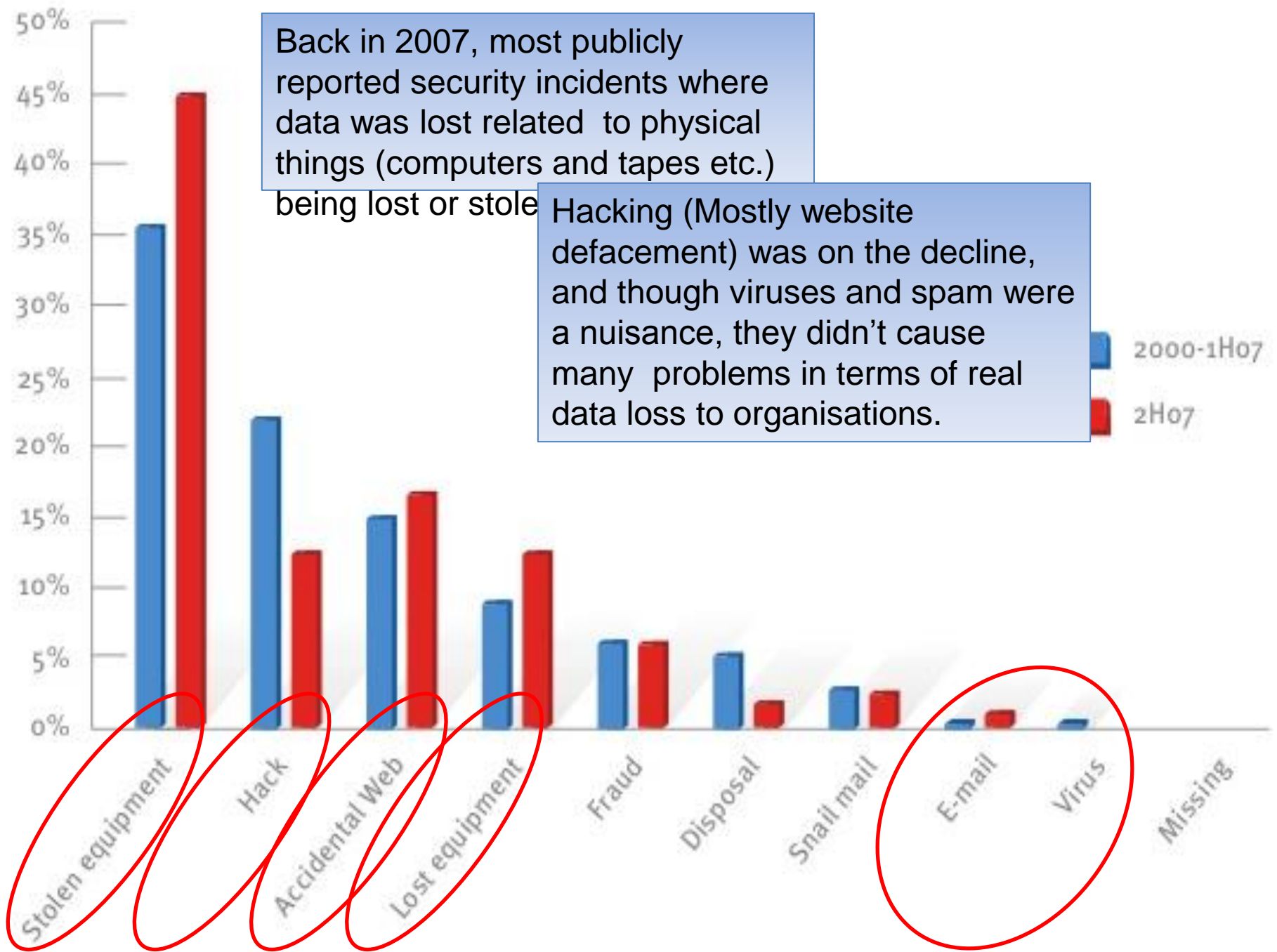


Figure 8. VERIS A<sup>4</sup> Grid depicting the frequency of high-level threat events

		Malware			Hacking			Social		Misuse	Physical
		Ext	Int	Prt	Ext	Int	Prt	Ext	Int		
Servers	Confidentiality & Possession	381			518						
	Integrity & Authenticity	397			422						
	Availability & Utility	2			6						
Networks	Confidentiality & Possession									1	
	Integrity & Authenticity	1								1	
	Availability & Utility	1								1	
User Devices	Confidentiality & Possession	356								1	86
	Integrity & Authenticity	355									86
	Availability & Utility									1	3
Offline Data	Confidentiality & Possession									23	
	Integrity & Authenticity										
	Availability & Utility										
People	Confidentiality & Possession							30	1		
	Integrity & Authenticity							59	2		
	Availability & Utility										

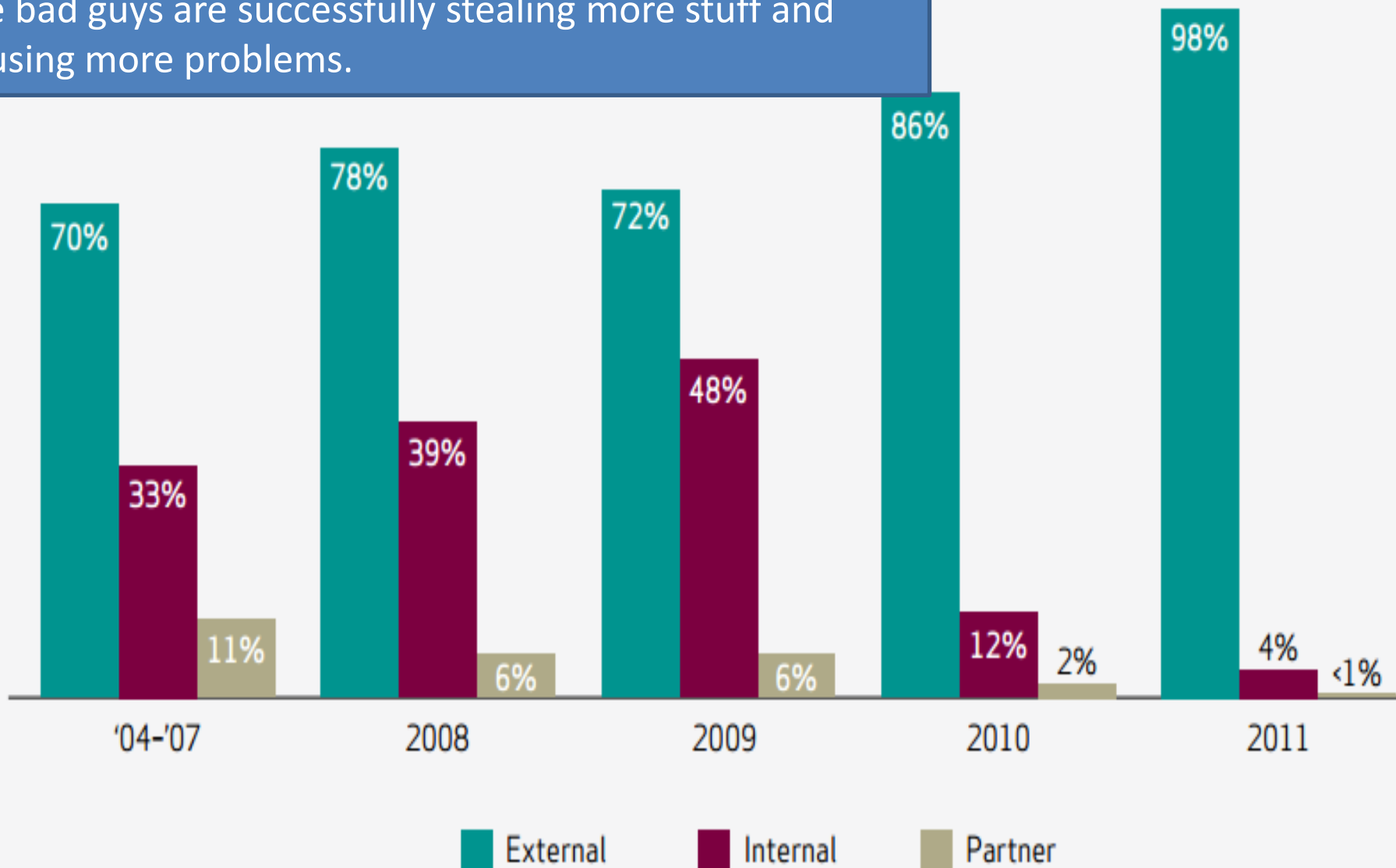
Viruses (malware) and hacking, targeting both end users and servers are the dominant cause of reportable data loss.

Loss or theft of end user devices (laptops, phones etc.) remains an issue.

Phishing is now a significant problem

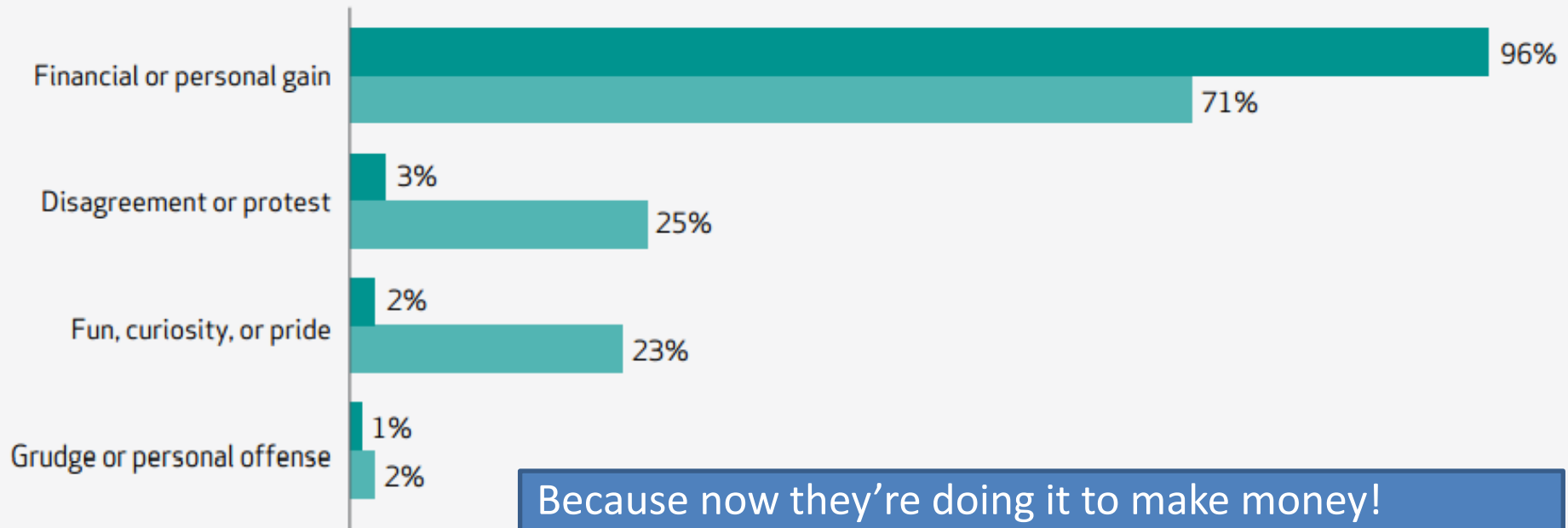
Or, to put it another way..

In both absolute terms (lots more incidents reported), and relative terms (bigger share of reported incidents), the bad guys are successfully stealing more stuff and causing more problems.



# Why?

Figure 15. Motive of external agents by percent of breaches within external



Because now they're doing it to make money!

Big organisations are still targeted for non-financial reasons- protests and pride.

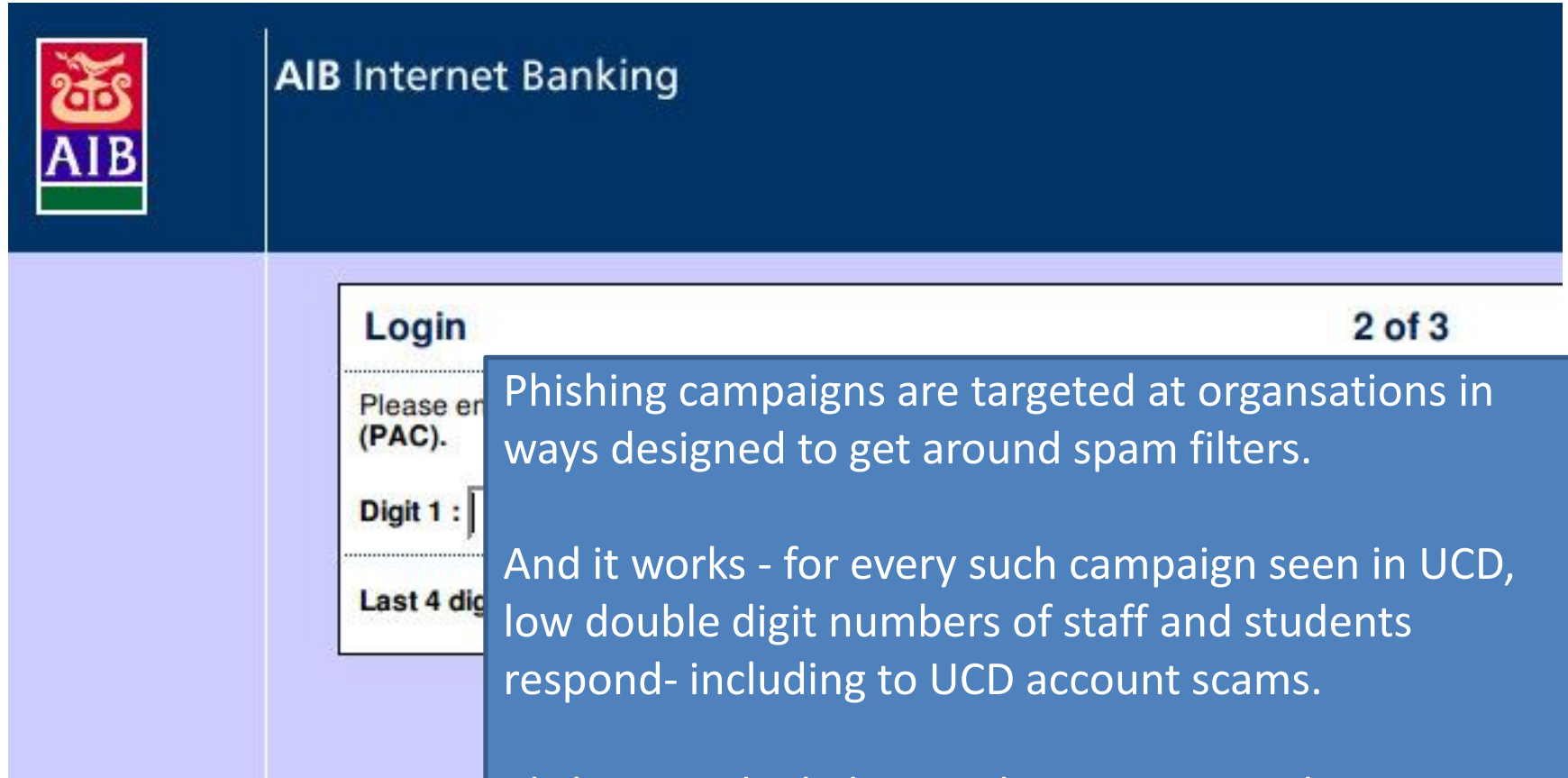
Note: In this sample, UCD doesn't qualify as "big" - think Boeing, Siemens, Nestlé ..

# How do I get someone's password?

- Ask them nicely, threaten them?
  - E.g. Phishing email
  - Helpdesk call
  - Survey
  - Chocolate bar
- How do I get anyone's password
  - Dictionary attack- make lots of guesses.
  - Get into the server (hacking)

And we're seeing this too..

# Attack type 1: Phishing

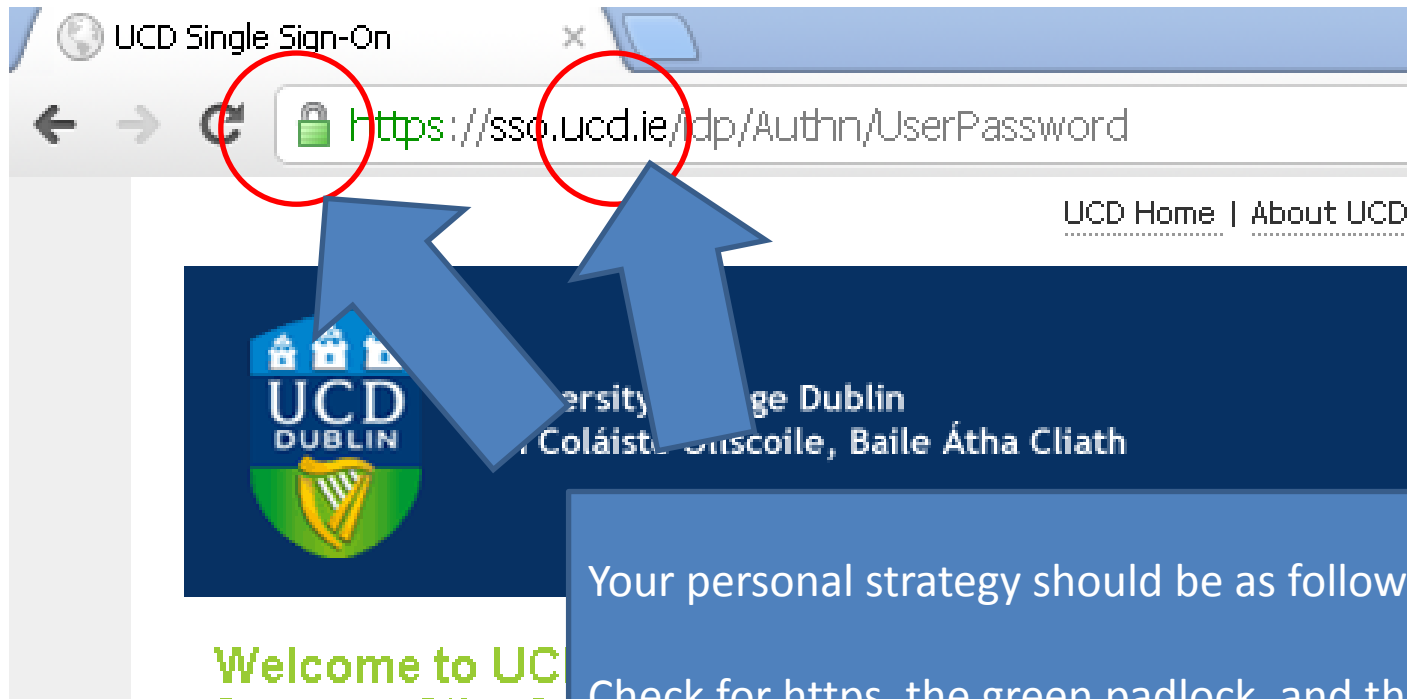


Phishing campaigns are targeted at organisations in ways designed to get around spam filters.

And it works - for every such campaign seen in UCD, low double digit numbers of staff and students respond- including to UCD account scams.

Clicking on the link can take you to a site hosting malware, ask you to “confirm” bank or credit card details, or request your UCD credentials.



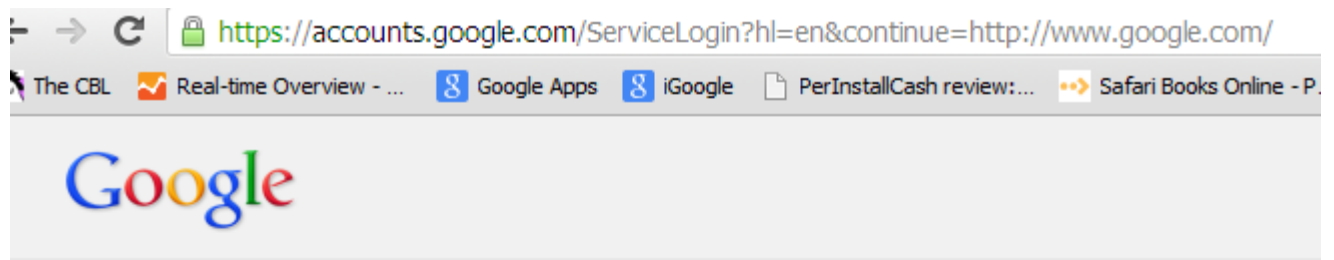


Your personal strategy should be as follows:

Check for https, the green padlock, and the last part of the server hostname is ucd.ie.

And all of this in the title bar of the web page-  
everywhere else it can be faked.

Never ever enter your UCD password on a non-UCD site . (By the way, this includes Google)



## Accounts

When you log in to Google,  
Never enter your UCD password.

When you click on “Sign in”

It takes you to a UCD service called Single sign on,  
where you can enter your password safely.

Google Account.

important email.

our past searches.

Sign in

Email

joe.bloggs@ucd.ie

Password

|

Sign in

☐ Stay si

[Can't access your account](#)

# Attack 2: Password Cracking...



In June 2012, LinkedIn contacted all its users and asked them to change their password, because encrypted copies of the password database had been uploaded to hacker sites.

-They're a visible victim of a new trend in password cracking

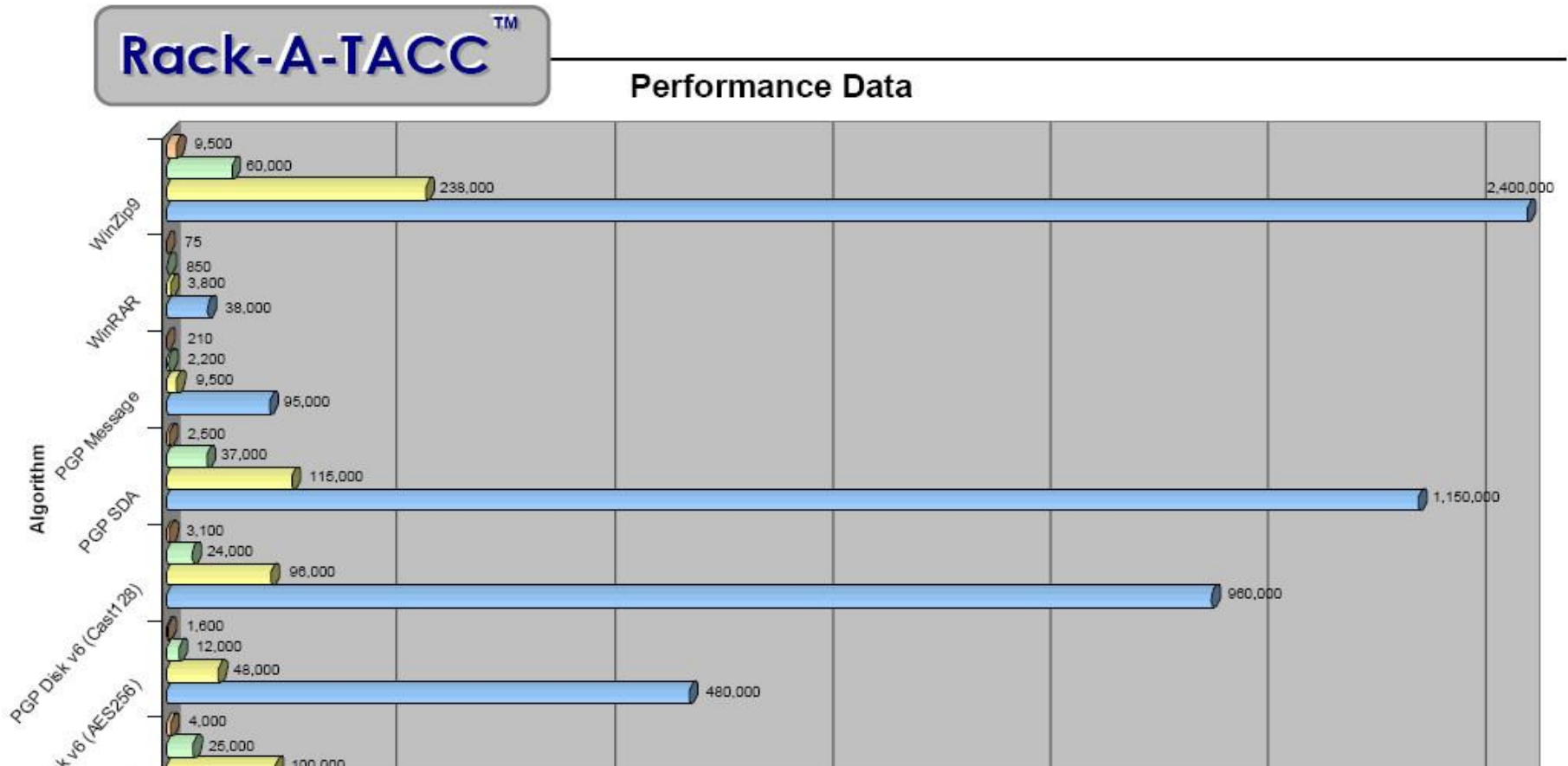
By the way, Linkedin user..

Was your password the same as  
your UCD one?

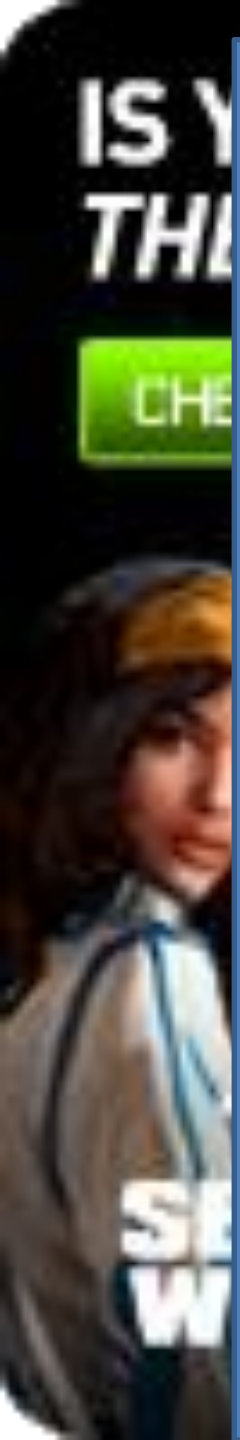
# Back in the day (2010 )

Password cracker - €100k buys a system that can test 2.4 million passwords\sec.

Only available to law enforcement\military.



What's changed?



Today, Graphics cards for PC gaming have 10x- 20x the computational power of a main CPU for number crunching problems.

Freely available password cracking software has been optimised to use this capability in systems with one or more such cards.

Encrypted passwords can often be harvested from sites and/or networks from web traffic.

Hackers use graphics cards to crack passwords to pay for new graphics cards- bounties are in the tens of dollars per password for one-offs.

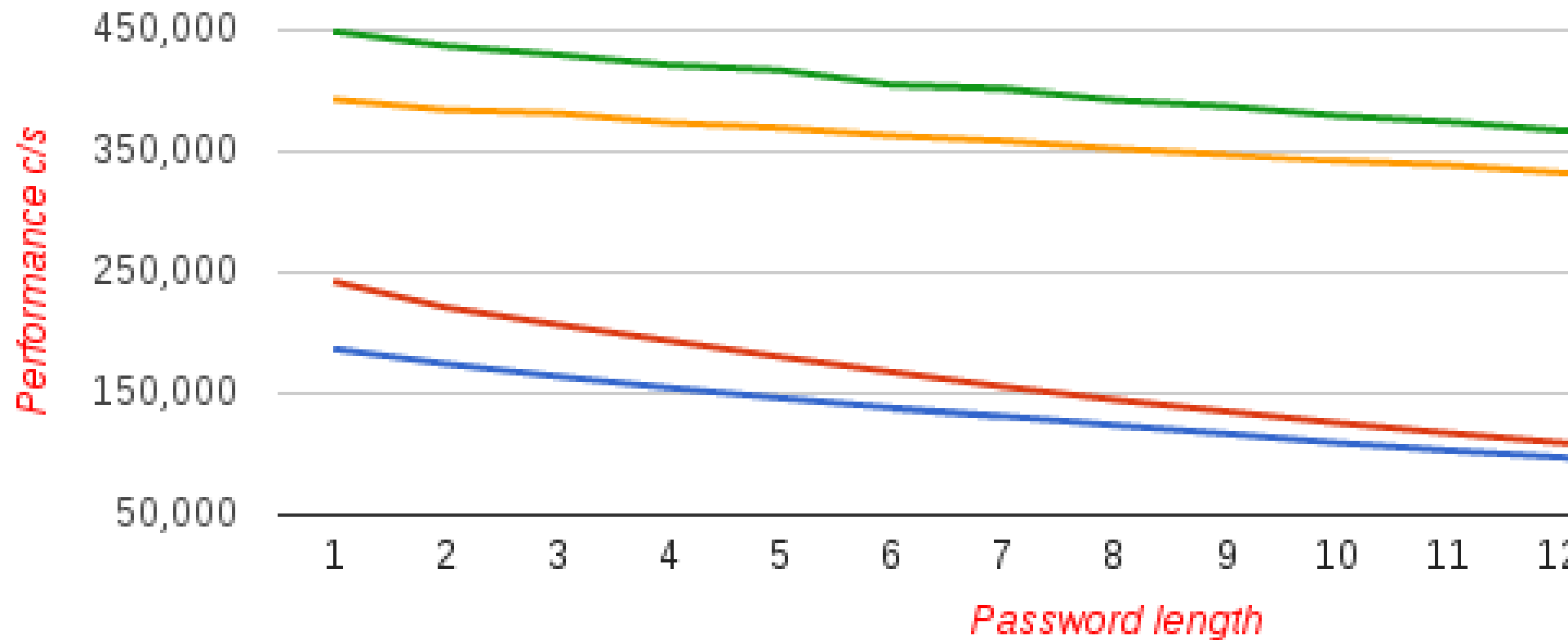
=> Thriving economy in password cracking by game-playing hackers...

# Benchmark- 400,000 checks/sec

€200 graphics card for a PC System

Costs for 2.4m pw/sec system is <=€2k with off the shelf hardware

**John The Ripper MD5-crypt CUDA Performance [28bl:512th,384 for rev**





So far, so bad

Is there any hope?

# Yes- Picking Safe Passwords



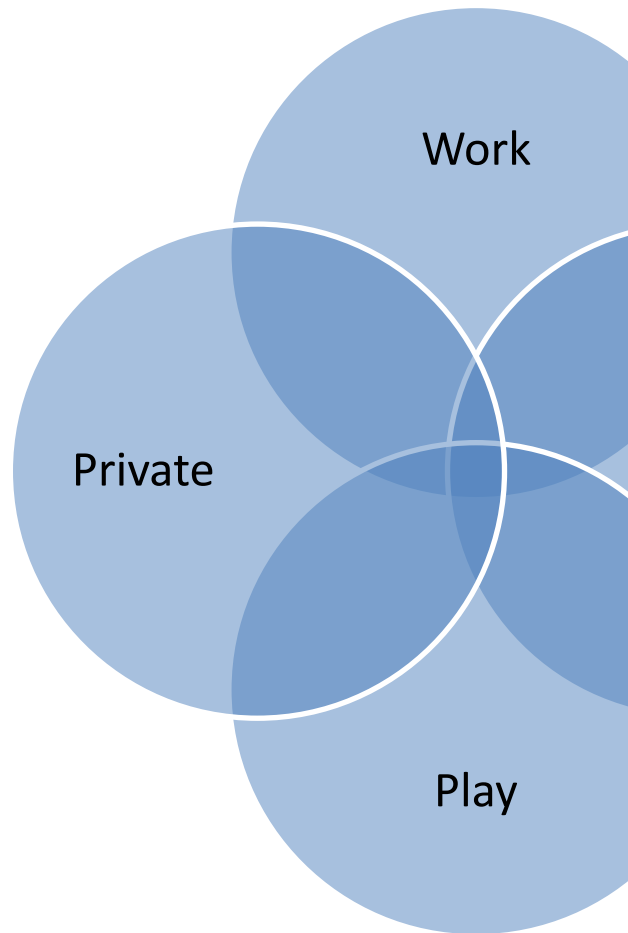
# What you've probably heard

- You should have different passwords for every system.
- Change them frequently- monthly.
- Make sure it's random and has letters, numbers and symbols.
- Never write them down!

# But what we know is:

- Most people have a few cherished password “friends”..
- Use them for everything.
- And never change them.

# Practical strategy- Personas and passwords



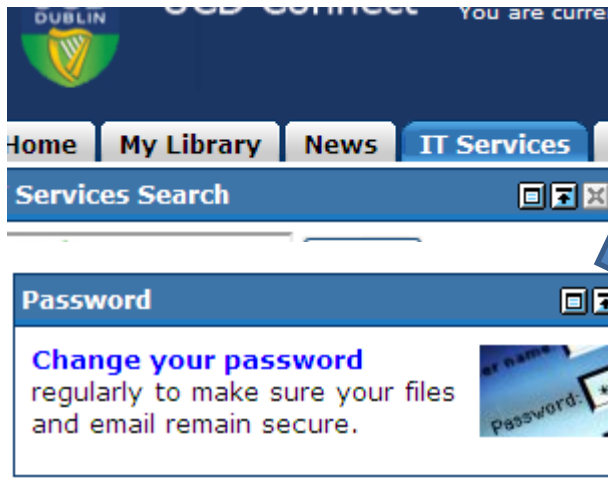
Have separate passwords for the different aspects of your life:

Never use your UCD password for non-UCD systems.

You don't have to change passwords frequently, but change regularly - like your toothbrush, not your car!

Have a disposable email account and password just for websites that you don't care about (i.e. Ones that don't have your credit card details)

# How to change your password for UCD Connect\ Novell



Log in to Connect  
and click here...

Or go to this webpage



# Password selection

- Choose a Phrase
  - E.g. "To be or not to be, that is the question."
- Take the first letter from each word, and keep capitals and punctuation.
  - Tbontb,titq.
- Change one or two characters to numbers (don't get too creative!):
  - Tbontb,t1t9.
- The target length should be 10+ characters
- Think Passphrase not password



# Summary

- Your passwords protect important data.
- Keep them separate and secure
- Choose them wisely.
  - Think *PassPhrase*, not *Password*
- Change them regularly

So, What else happens?

## Today's landscape for web threats

Here are just a few of the techniques cybercriminals commonly use to distribute malware on the web:



**Blackhat search engine optimization (SEO)** ranks malware pages highly in search results.



**Social engineered click-jacking** tricks users into clicking on innocent-looking webpages.



**Spearphishing sites** mimic legitimate institutions, such as banks, in an attempt to steal account login credentials.



**Malvertising** embeds malware in ad networks that display across hundreds of legitimate, high-traffic sites.



**Compromised legitimate websites** host embedded malware that spreads to unsuspecting visitors.



**Drive-by downloads** exploit flaws in browser software to install malware just by visiting a webpage.

Malicious code typically installs spyware or malware by exploiting known vulnerabilities in your browser or associated plugins. These malware threats include:



**Fake antivirus** to extort money from the victim.



**Keyloggers** to capture personal information and account passwords for identity or financial theft.



**Botnet software** to subvert the system into silently joining a network that distributes spam, hosts illegal content or serves malware.

# UCD Risk Events

- Daily events
  - Laptop theft
  - Account Compromise (virus\hacker)
  - Computer Compromise (>300 in 2011)
  - Loss of single\folders of documents.
- Routine events
  - Personal bank\ credit card account compromise.
  - Server hacked.
  - Lost all data on server\computer.
  - Lost all data\ research group server.
  - Loss of backup material.

# Limits of Technology

- Computers are good at:
  - Consistent response
  - Predictable behaviour
  - Displaying data
  - Facilitating analysis
  - Storing and processing data.
- Computers are bad at:
  - Making decisions with incomplete information.
  - Interpreting language.
  - Making Trust decisions.
  - Spotting Deception

# Human Factors

# Spotting Fake websites



## Tax Refund - About You

(\*) Indicates a required field.

### Personal Details

First Name:	*	<input type="text"/>
Surname:	*	<input type="text"/>
Date of Birth:	*	Day <input type="text"/> Month <input type="text"/> Year <input type="text"/>
Mother's Maiden Surname:	*	<input type="text"/>

### Address

**IMPORTANT:** Please select your county from the list provided. Do not type the county in any of the fields Address Line 1 - 3.

Address:	*	<input type="text"/>
City	*	<input type="text"/>
County:	*	<input type="text"/>

### Contact Details

Daytime Phone Number:	*	Area Code <input type="text"/>	Local Number <input type="text"/>
Email:	*	<input type="text"/>	

Continue

# Indicators of fraud- communication

- Email with links.
- Urgent action.
- Explicit or implied threat of loss.
- Unexpected communication.
- No opportunity to check.
- “Ingrish” or bad grammar.

Dear Applicant:



After the last annual calculation of your fiscal activity we have determined that you are eligible to receive a tax refund of **281.23 EURO**.

Please submit the tax refund and allow us 3-9 business days in order to process it.

If you don't receive your refund within 9 business days from the original Revenue - Irish Tax & customs mailing date shown on *Where's My Refund?*, you can start a refund trace online.

To get to your personal refund information, be ready to enter your:

- Filing status (Single, Married Filing Joint Return, Married Filing Separate Return, Head of Household, or Qualifying Widow(er))
- Your Date of Birth
- Full name, Address, Phone and the Credit/Debit Card where refunds will be made.

To access the form for your tax refund, please click on the "*Where's My Refund?*" above image or [Tax Refund Online Form](#)

**Note:**

- For security reasons, we will record your ip-address and date.
- Deliberate wrong inputs are criminally pursued and indicted.



# Trust this?

- Phishing works. It's a probability game.
- They get better all the time.
  - “Ingrish” spotting isn't enough anymore.
- Good browser tools from:
- Google (Built into chrome)
- McAfee- Siteadvisor (free plugin for most browsers)

# Problem- establishing trust

## Physical World.

- Physical location.
- Look and feel of premises.
- Staff attitude.
- Reputation.
  
- Physical world is solid and expensive to generate=
- lots of strong trust cues available.

## Internet World.

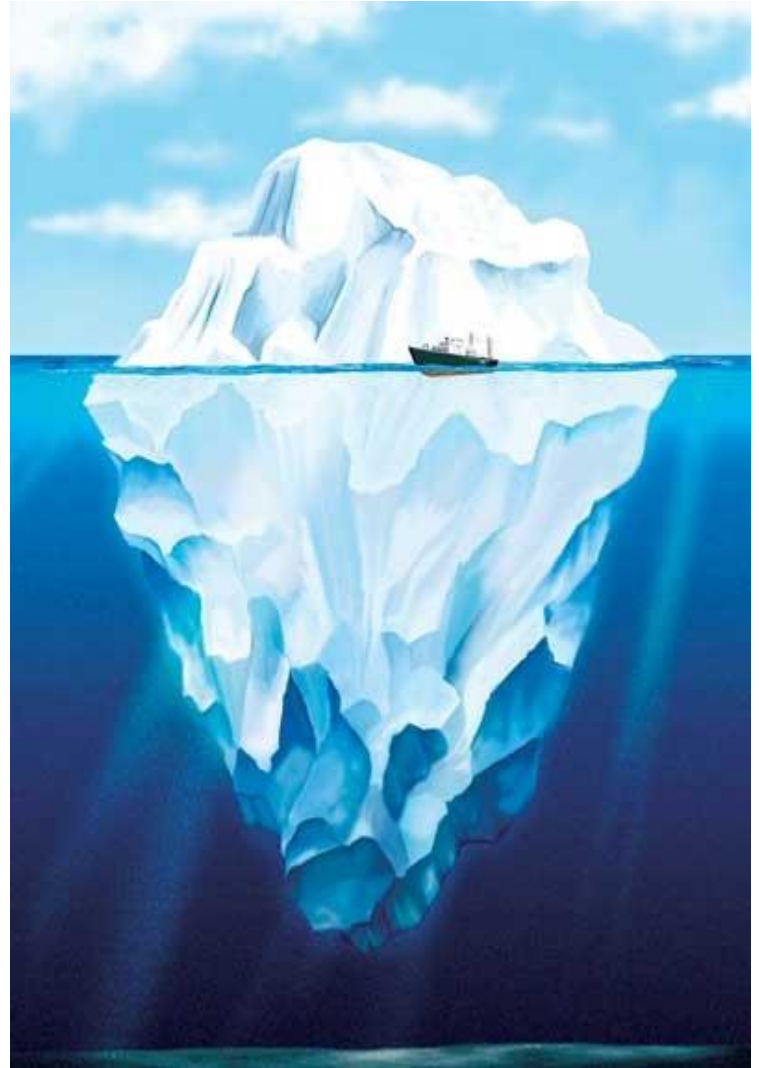
- Everything is just pictures and text.
- Most things can be faked or reproduced easily.
- Reputation is only valuable if it can't be duplicated.
  
- Weak native basis for trust.

# Ask yourself these..

Am I comfortable with this?

Why are they lying to me?

Why do I have to do this  
now?



# Spotting Deception attacks

## (By whatever source)

- Urgent.
- Threaten consequences.
- Invoke authority.
- Claim to be insider.
- Might really be insider but unauthorised.
- Name drop
- “Story!”
- Influence attacks:
  - Reciprocation.
  - Consistency.
  - Affinity.

# Response to deception

- I feel uncomfortable=  
There is a problem.
  - Take a number to call back.
  - Take time to think.
  - Take time to check.
- Get specifics.
- Wait for threat.
- Watch for story.
- Remember, it could be real!
- Stay polite.
- Recognise importance and urgency for caller.
- Ask them for checkable facts.

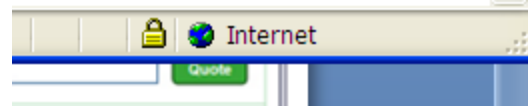
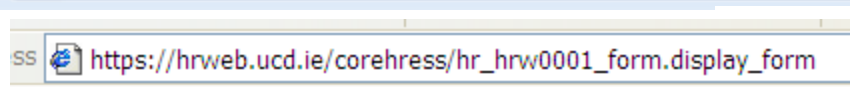
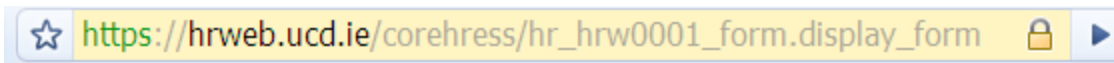
# Trust cues- What you see isn't necessarily real!

- Good checks for site:

- “Padlock”- where?
  - The address bar?
  - The status bar?
  - What does it mean?
- Https:// (in green is good)
- Site name is correct.

- Bad checks:

- Security “Brand” marks
- “Hacker safe” etc.
- Ever heard of these companies?
- Padlocks on the web page itself.
- Waffle text about security.



# Real or fake?

Trade Broker Online - Microsoft Internet Explorer

File Edit View Favorites Tools Help

https://www.tradebrokeronline.com/tradestocks

Trade Broker Online

## TradeBroker Online

Trading & Investing | Quotes & Research | Retirement & Planning | Banking & Lending

Trade | My Accounts | My Quotes | Order History | Extended Hours Trading | IPO Center

Stocks | Options | Mutual Funds | Bonds | Customer Offerings

Account: 223-5213-6343-01 [Open Orders](#)

Order Type: Buy

Shares:

Symbol:

Price Type: Market

Term: Good for day

[Place Order](#)

System response and account access times may vary due to a variety of factors, including trading volumes, market conditions, system performance, and other factors. Trade Broker Online, Inc. reserves the right to reject market orders, block size orders and orders for securities traded in a thin market. [Learn more.](#)

### Account Balance

Cash Balance:	\$10,000.00
Margin Balance:	\$2,322.53
Money Market Balance:	\$25,683.10
Funds Available Cash Trading:	\$10,000.00
Funds Available Margin Trading:	\$2,322.53

### Quotes

▼ DJIA	10,216.91	-36.26	-0.4%
▼ NASDAQ	2,037.47	-23.62	-1.1%
▼ S&P 500	1,177.68	-7.19	-0.6%

MARKET DATA DELAYED AT LEAST 20 MIN

[More Market Info](#)

[Contact Us](#) | [Site Map](#) | [Privacy & Security](#) | [About TradeBroker Online](#) | [Careers](#) | [Legal Information](#)

© 2005 TradeBroker Online, Inc. All rights reserved.  
Brokerage Products: Not FDIC-Insured/No Bank Guarantee/May Lose Value

Local intranet

Trade Broker Online - Microsoft Internet Explorer

File Edit View Favorites Tools Help

http://www.tradebrokeronline.com/tradestocks

Trade Broker Online

## TradeBroker Online

Trading & Investing | Quotes & Research | Retirement & Planning | Banking & Lending

Trade | My Accounts | My Quotes | Order History | Extended Hours Trading | IPO Center

Stocks | Options | Mutual Funds | Bonds | Customer Offerings

Account: 223-5213-6343-01 [Open Orders](#)

Order Type: Buy

Shares:

Symbol:

Price Type: Market

Term: Good for day

[Place Order](#)

System response and account access times may vary due to a variety of factors, including trading volumes, market conditions, system performance, and other factors. Trade Broker Online, Inc. reserves the right to reject market orders, block size orders and orders for securities traded in a thin market. [Learn more.](#)

### Account Balance

Cash Balance:	\$10,000.00
Margin Balance:	\$2,322.53
Money Market Balance:	\$25,683.10
Funds Available Cash Trading:	\$10,000.00
Funds Available Margin Trading:	\$2,322.53

### Quotes

▼ DJIA	10,216.91	-36.26	-0.4%
▼ NASDAQ	2,037.47	-23.62	-1.1%
▼ S&P 500	1,177.68	-7.19	-0.6%

MARKET DATA DELAYED AT LEAST 20 MIN

[More Market Info](#)

[Contact Us](#) | [Site Map](#) | [Privacy & Security](#) | [About TradeBroker Online](#) | [Careers](#) | [Legal Information](#)

© 2005 TradeBroker Online, Inc. All rights reserved.  
Brokerage Products: Not FDIC-Insured/No Bank Guarantee/May Lose Value

Local intranet

# What should I do?

## Personal Plan- Security is Routine!

- Things I do every day
- Things I do weekly
- Things I do quarterly
- Things I do when the situation arises-
  - New Computer
  - Recycle computer
  - Something bad happens



# Most important

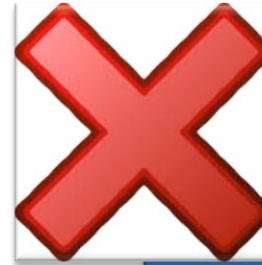
- Regular tasks
  - Get your computer set up correctly.
    - Sophos AV, Admin Password, Updates and Firewall
  - Set and protect strong passwords. Change them regularly.
  - Use email and the internet securely.
  - Back up your data.
  - Lock your screen every time you leave your computer.
- Ask for help when you need it!

# Backing up data



## Good choices

- Novell Fileshares
- Connect MyFiles
- Google Docs\Drive
- Spideroak



## Bad Choices

- Dropbox
- Local storage
- USB Drives

# I have a laptop..

- Don't share it (especially at home).
- Put a visible asset tag on it.
- In cars- Keep it in the boot only.
- Get it encrypted if you manage sensitive data.
- Vehicles, Airport, hotel, restaurant, public areas are high theft areas.
- Children, food, spouses are high data-loss scenarios.

# I have a smartphone

- If it has access to UCD data, (including email) it must have a PIN for access.
- If it stores data, the device must be set up to use encryption. (e.g. Standard option in iTunes sync, methods vary with android)
- Strongly recommend users enable remote lock\remote wipe features in case device is lost.

# Everyday scenarios

- I need access to my colleagues account\computer.
  - Written approval from Head of school\Unit plus account details issued to HR Partner.
- I look after someone else's email.
  - They can delegate access through Gmail.
- I need to access a business system from home.
  - Use VPN and UCD computer

# Everyday tasks

- Clear desk of sensitive material
  - At the end of the day- lock it away!
- Lock screen when leaving desk-
  - Windows Button + L
- Back up your data.
  - Network share, email, Connect files
- Leave time for Updates
- Log out and shut down when leaving work

# Weekly tasks

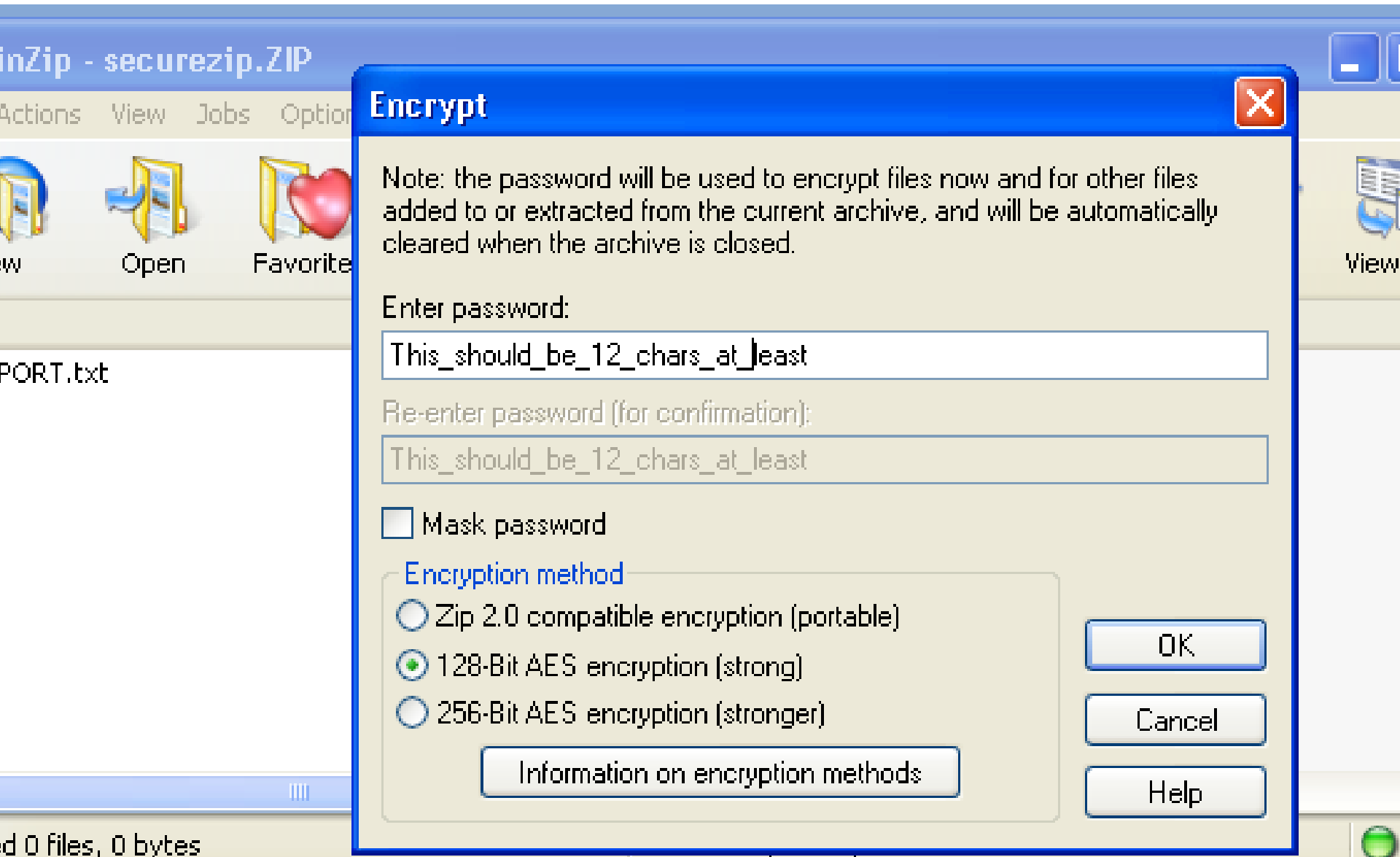
- Run a virus scan
- Check a backup
- Check your updates
- Read the announcements page.

# Encryption

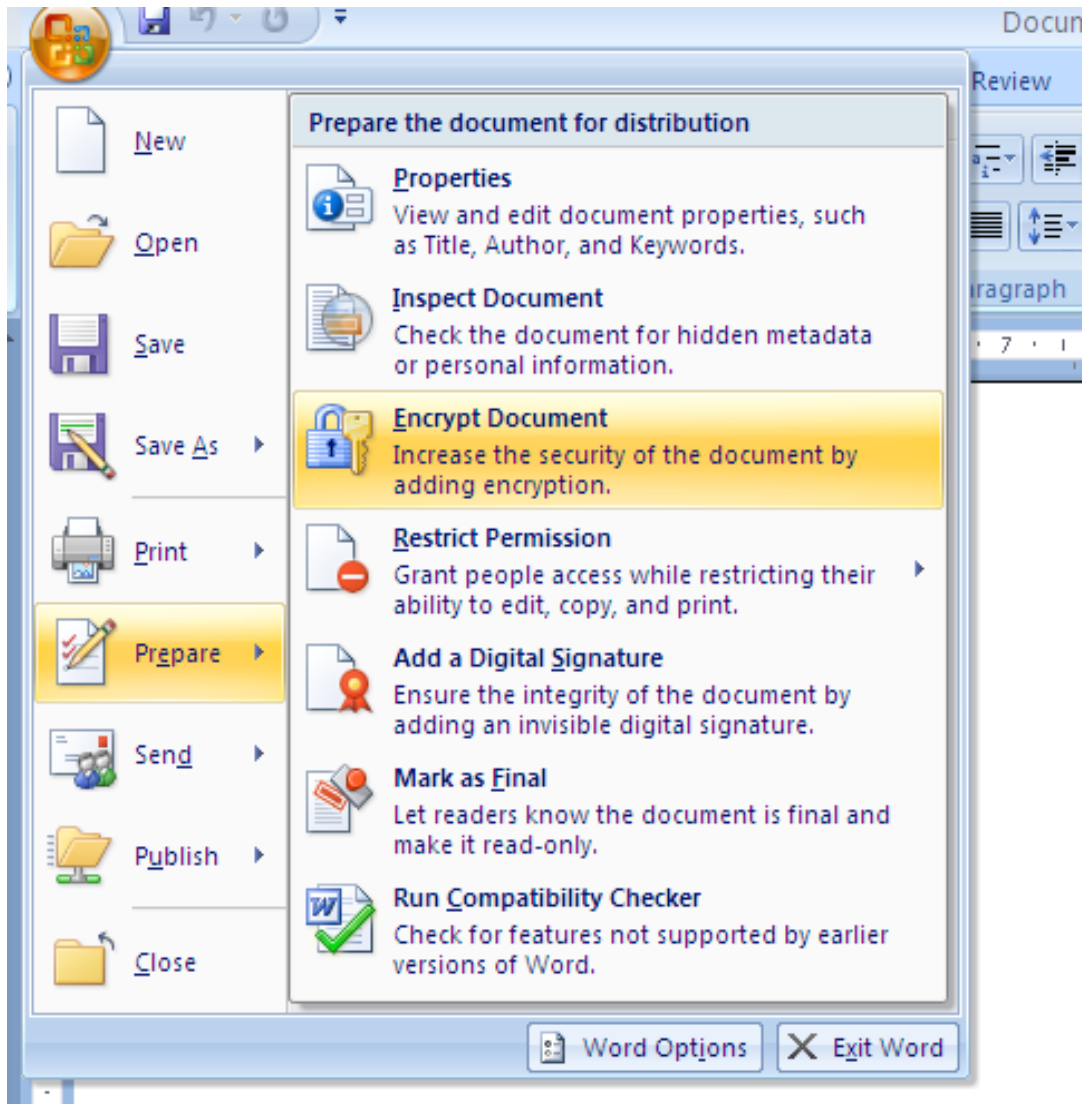
- Data on device
- Data for sharing
  - Email or file share
- Communicating passwords
  - By project\relationship
  - Doesn't work for large groups.



# Using Winzip securely



# Passwords and office



- Office 2007+
- Password protect COPY of document to share.
- Never email passwords-
- Inform by phone or text

# Browsers and Web applications

- When finished with a computer, always exit the browser completely.
- Applications and sessions are usually stored in browsers even if a window isn't currently open.
- UCD Single sign on stays working as long as any browser window is open.

# Seek Help for:

- All use of encryption.
- Disposing of computers or devices with sensitive data.
- Setting up a secure machine for use with sensitive data.
- If you think you have a virus.
- If you think there's been an incident.

# Seeking help

- [www.ucd.ie/itservices/itsecurity](http://www.ucd.ie/itservices/itsecurity)
  - Today's material.
  - UCD data handling policy
  - UCD Administrative Security policy
- UCD Helpdesk
  - 2700
  - [ithelpdesk@ucd.ie](mailto:ithelpdesk@ucd.ie)
- Sensitive incidents
  - [John.curran@ucd.ie](mailto:John.curran@ucd.ie)
  - [Ciara.acton@ucd.ie](mailto:Ciara.acton@ucd.ie)