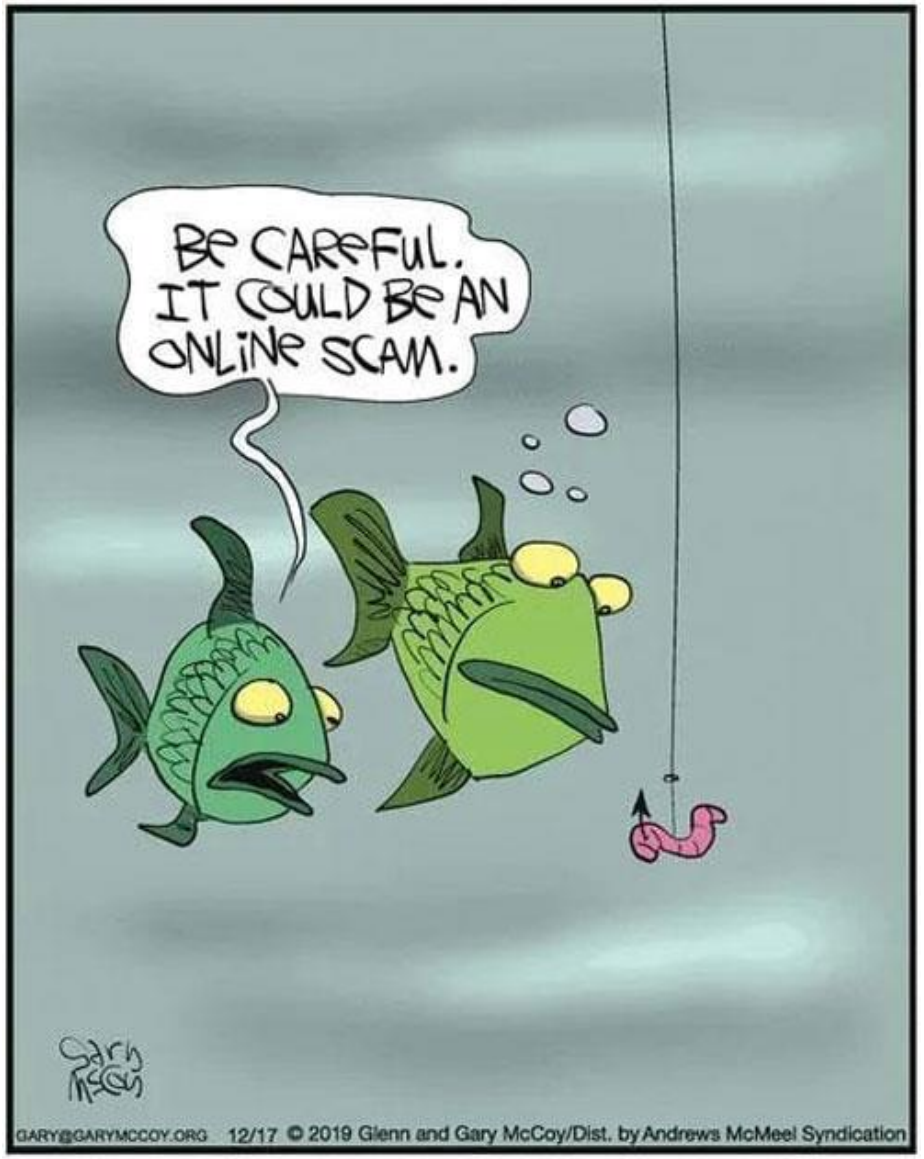
COMP1710/6780
A bit more about cybersecurity:
botnets, tracking and
social engineering (spoofing, phishing and spam)



vulnerabilities

A vulnerability is a weakness in an application that may allow a malicious entity to cause harm

Vulnerabilities are generally caused by a design flaw or implementation bug

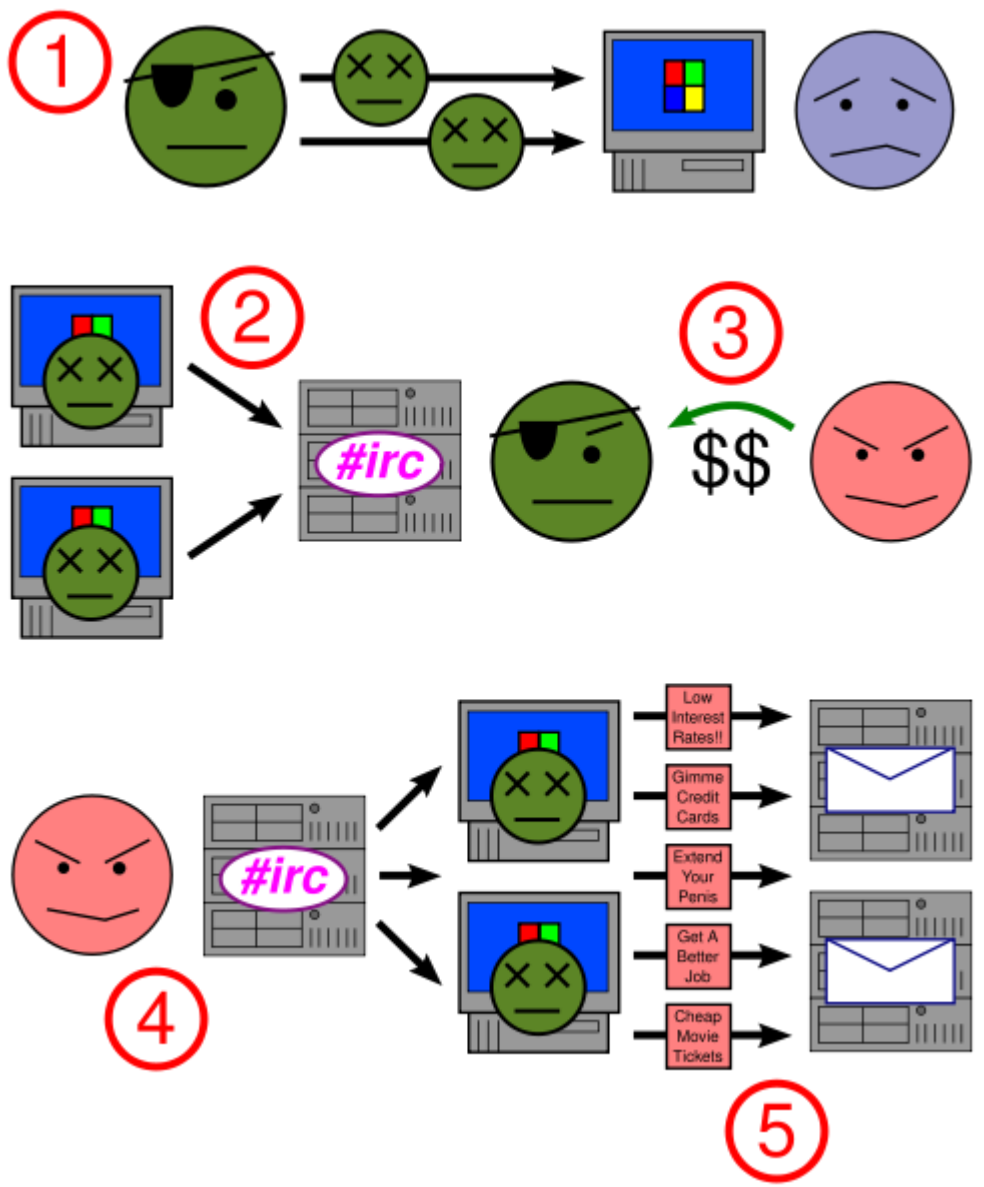
Again: new vulnerabilities are discovered daily!

Evelyn Simak / Gap in fence

Bot: Internet bot, web robot, robot

1. A botnet operator sends out viruses or worms, infecting ordinary users' computers, whose payload is a malicious application – the bot.
2. The bot on the infected PC logs into a particular Internet Relay Chat (IRC) server (or in some cases a web server). That server is known as the command-and-control server (C&C).
3. A spammer purchases access to the botnet from the operator.
4. The spammer sends instructions via the IRC server to the infected PCs, …
5. … causing them to send out spam messages to mail servers.

A bot is sometimes called a 'zombie' and a botnet a 'zombie army'



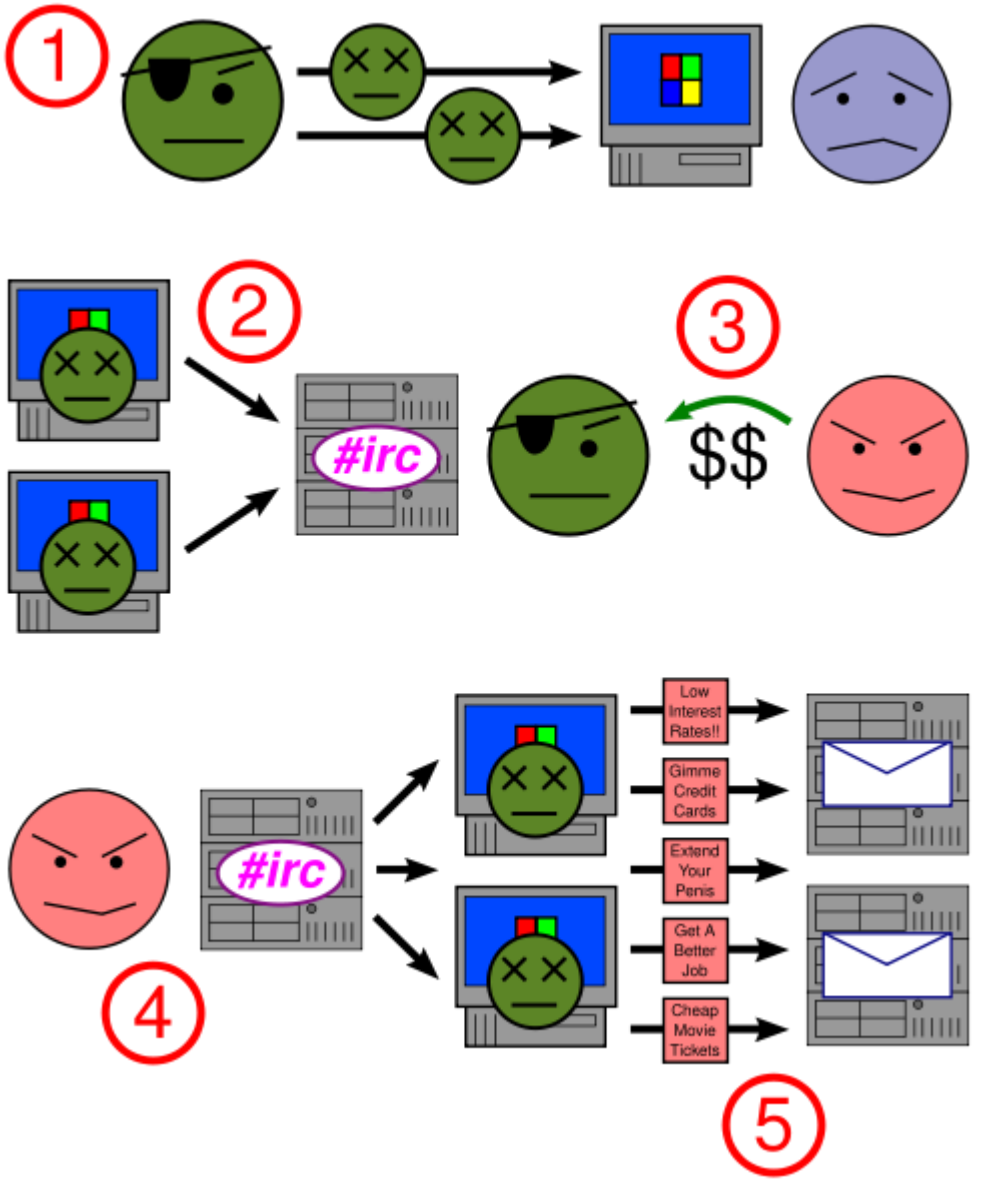
Uses of a botnet

Botnets are exploited for various purposes, including:

- denial-of-service attacks,
- creation or misuse of SMTP mail relays for spam (see Spambot),
- click fraud,
- spamdexing and
- the theft of application serial numbers, login IDs, and financial information such as credit card numbers

Simple Mail Transfer Protocol

Filling index.html files with words and links to manipulate search engine recognition



Uses of a botnet

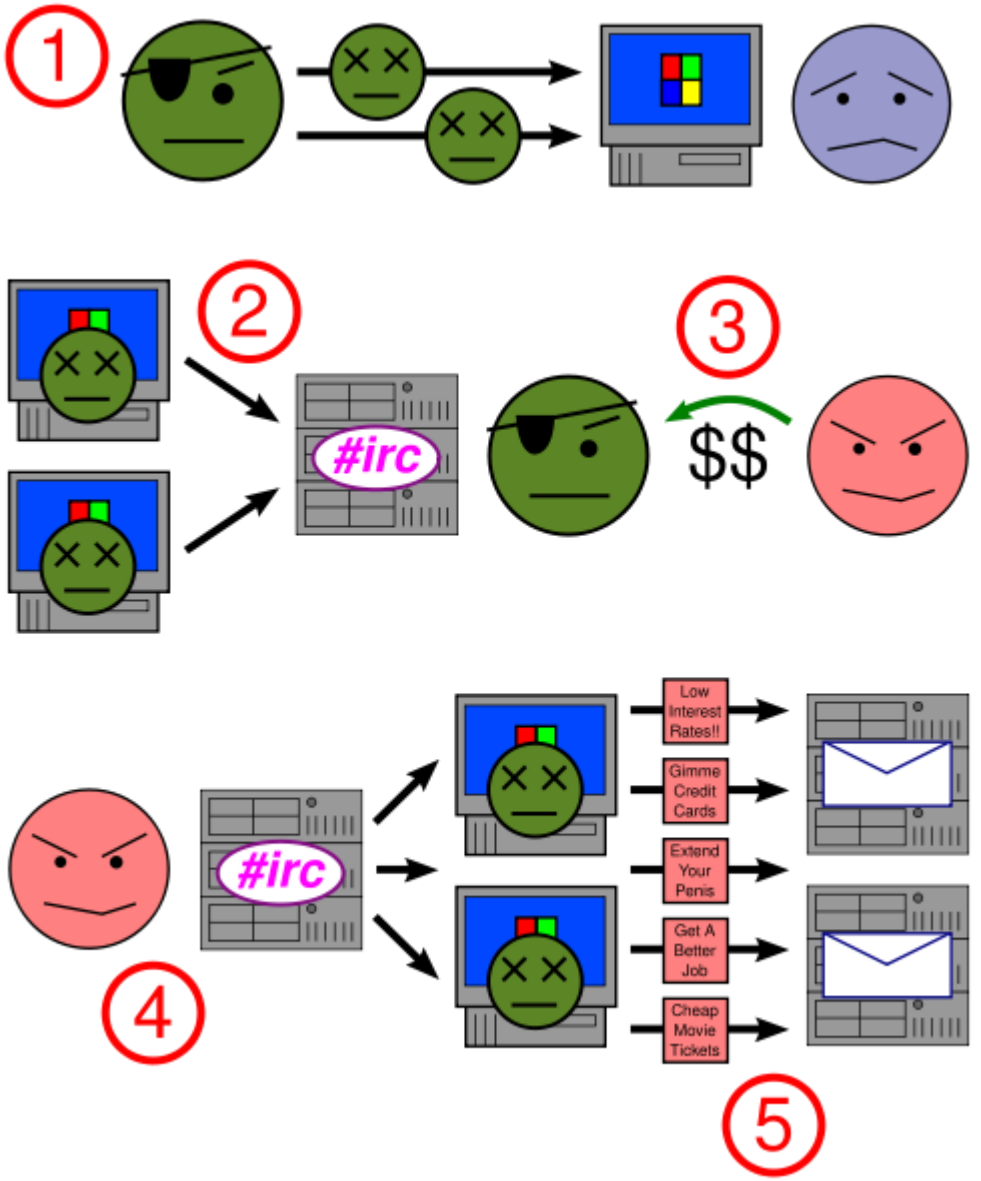
Denial-of-service attack where multiple systems autonomously access a single Internet system or service in a way that appears legit, but much more frequently than normal use and cause the system to become busy.

Adware exists to advertise some commercial entity actively and without the user's permission or awareness.

Spyware is software which sends information to its creators about a user's activities.

E-mail spam are e-mail messages disguised as messages from people, but are either advertising, annoying, or malicious in nature.

Click fraud is the user's computer visiting websites without the user's awareness to create false web traffic for the purpose of personal or commercial gain.



What can you do?

Learn and understand

Code securely; be aware of security implications

Test your code as part of the web development process

Defence in depth

Take a layered defence-in-depth approach

Set strong security policies and procedures, raise user education and awareness, and plan ahead

Implement physical doors and locks

Set effective firewall rules and router configurations

Segment your network and use intrusion detection systems

Update your operating system and use virus protection

Update your applications and develop security in

Use encryption and strong passwords

Policies
Physical Security
Perimeter
Internal Network
Host
Application
Data

What is tracking? Beyond 'cookies'

When people think of tracking, they think of 'cookies'.

Cookies are little strings of data (value pairs) that are passed along as you browse, and can be shared by ad networks. And ad networks are sharing their cookie information with each other.

You can clear your cookies

But there are many (and often sneaky) trackers 1,100+ identified trackers

Google Analytics tracking coverage is an estimated 46% of the web, they track Users by a ClientID, Bounce Rate, Sessions, Session Durations, etc.

Dual purpose widgets – Facebook 'likes' are tracking you! Skype, Twitter, etc.

Are you being tracked?

Fingerprinted: What browser, your fonts, timezone, screen size and colour depth, DNT Header enable?

Example: My Desktop

Test	Result
Is your browser blocking tracking ads?	✗ no
Is your browser blocking invisible trackers?	✗ no
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticlick does not measure all forms of tracking and protection.

Your browser fingerprint **appears to be unique** among the 211,059 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.69 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting here.

Example: My Laptop

Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your blocker stop trackers that are included in the so-called "acceptable ads" whitelist?	✓ yes
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✓ yes
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticlick does not measure all forms of tracking and protection.

Your browser fingerprint **appears to be unique** among the 211,468 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.69 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting here.

Mainstream browsers with an anti-tracking policy

Mozilla Firefox

Apple Safari

Mainstream browsers with no anti-tracking policy

Google Chrome

Microsoft Internet Explorer

Defences against tracking, public positions against them

Users are the weakest link

Social engineering is the attempt to **gain information**, **access**, or **introduce unauthorised software** into the system through the manipulation of end users

Social engineering remains one of the biggest threats

Technical safeguards and layers are great but they are **meaningless if users forcibly override them** or intentionally ignore them

SPAM

Phishing

Spoofing

Spoofing

Masked URL

Subj:	**Your Bank of Oklahoma Account could be Suspended**
Date:	10/31/2005 9:17:23 PM W. Europe Standard Time
From:	department@bankofoklahoma.com
To:	rsutton603@aol.com

Sent from the Internet (Details)

BANK OF OKLAHOMA
You're Better Off At BOk!

Security Alert

Please note that Your Bank of Oklahoma Online Account is about to expire,or there is a problem with your information.In order for it to remain active,and update your information,please use the link below to proceed and Verify Your Account:

http://secure.bankofoklah oma.com/cgi-bin/dll87443/update/default.asp

Bank of Oklahoma Security Department
Thank you.

Please Note: Bank of Oklahoma always contacts its costumers about acount expiration.That is how we show our *quality* and *respect* to our clients.However your information are 100% safe in our 128-ssl dabatase.

Subj:	**Your Bank of Oklahoma Account could be Suspended**
Date:	10/31/2005 9:17:23 PM W. Europe Standard Time
From:	department@bankofoklahoma.com
To:	rsutton603@aol.com

Sent from the Internet (Details)

BANK OF OKLAHOMA
You're Better Off At BOk!

Security Alert

Please note that Your B
there is a problem with
your information,please use th
ur Account:

http://secure.bankofoklah oma.com/cgi-bin/dll87443/update/default.asp

Bank of Oklahoma Security Department
Thank you.

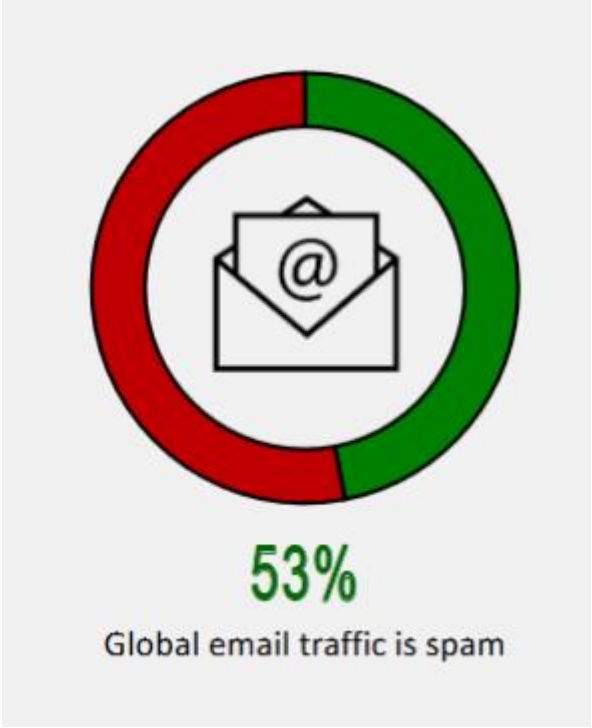
Please Note: Bank of Oklahoma always contacts its costumers about acount expiration.That is how we show our *quality* and *respect* to our clients.However your information are 100% safe in our 128-ssl dabatase.

Actually links to
http://212.45.13.185/bank/index.php

Cybersecurity - SPAM

[1] Parts of URL have been obscured to prevent accidental visitation of site

Spam and scams



Email dominates digital communication, presenting huge opportunity for circulating spam

- Can be harmless, but unsolicited or unwanted
- Often more malicious and serious
- Email based threats, malware, and phishing

Stat from Symantec

YOU SHOULD NEVER SPAM!

What is Spam?

Spam is a generic term used to describe electronic 'junk mail' – unwanted messages sent to your email account or mobile phone. These messages vary, but are essentially commercial and often annoying in their sheer volume. They may try to persuade you to buy a product or service, or visit a website where you can make purchases; or **they may attempt to trick you into divulging your bank account or credit card details**.

In Australia, spam is defined as 'unsolicited commercial electronic messaging'. New Australian legislation relating to spam – the Spam Act 2003 – came into effect on 10 April 2004. This consumer guide outlines the new law; it also offers practical advice on how you can reduce the amount of spam you receive, and suggestions on what to do when you receive spam

Unsolicited mail

SPAM = Stupid Pointless Annoying Messages (this is a *backronym*)

or SPAM = Seriously Pernicious and Malicious (my backronym)

Spam and scams

Spam according to the Australian Law: Spam Act 2003 – came into effect on 10 April 2004.

To comply with Australia's spam laws, a commercial electronic message must meet the following conditions. Any message sent to you that doesn't meet all three of these conditions is defined as spam:

- **Consent** - it must be sent with your consent. You may give express consent, or consent may be inferred from your conduct and 'existing business or other relationships'
- **Identify** - it must contain accurate information about the person or organisation that authorised the sending of the message
- **Unsubscribe** - it must contain a functional 'unsubscribe' facility to allow you to opt out from receiving messages from that source in the future

A spam message is not necessarily sent out in 'bulk' to numerous addresses – under Australian law, a single electronic message can also be considered spam.

Exemptions

Electronic messages from certain sources are exempted from the legislation. These include messages from: government bodies, registered political parties, charities, religious organizations, educational institutions (sent to attending and former students and their households). See *Australian Communications and Media Authority* for more

Spam and scams

What is Phishing?

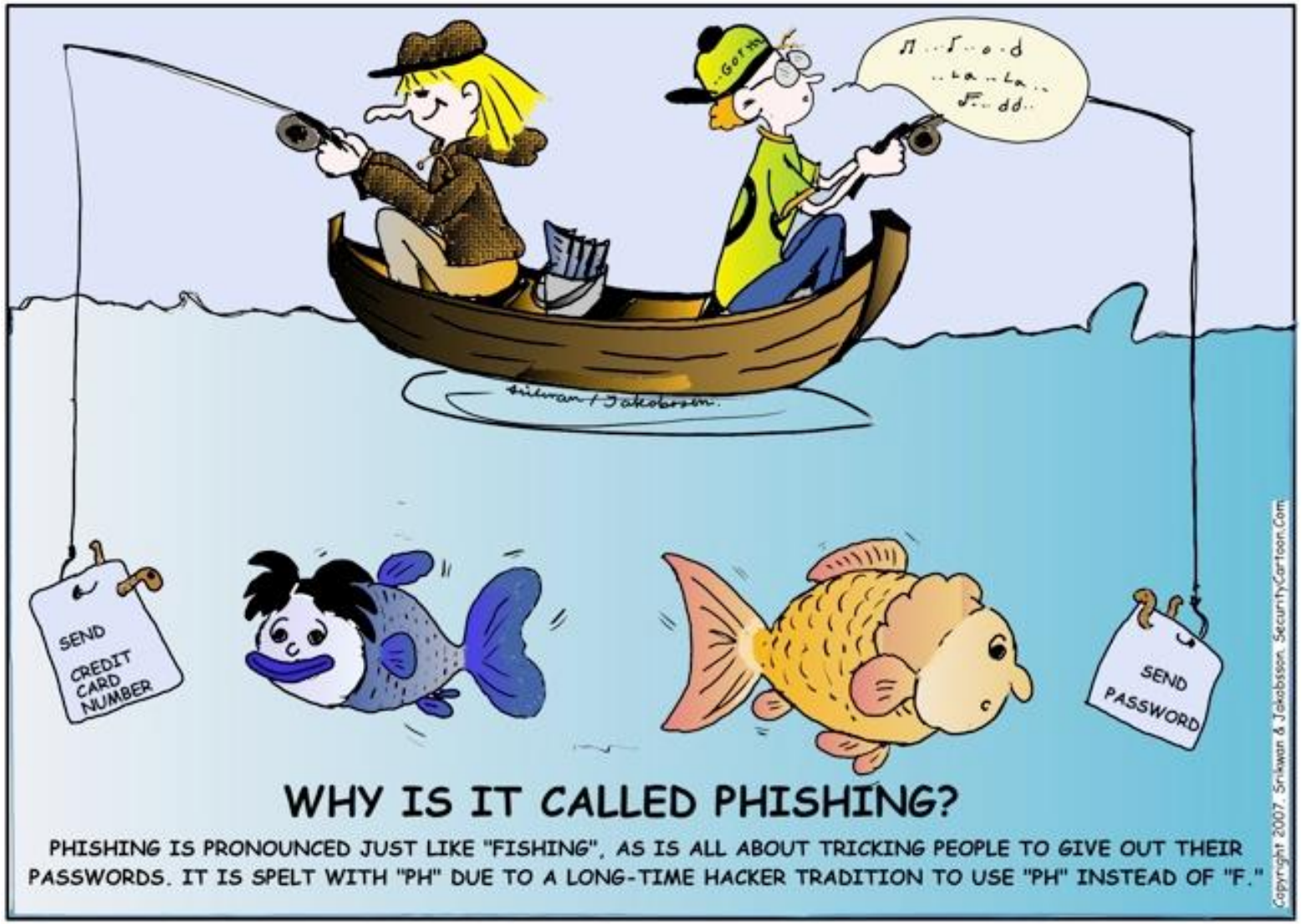
Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials

Anti-phishing Working Group

The total number of phishing attacks in **2016** was **1,220,523**, a 65% increase over 2015.

In **2019** phishing in social media ***doubled***.

In the second quarter of 2022,there were 1,097,811 attacks observed, so est. **~4 million** phishing attacks for **2022**



What is Phishing (continued)?

Social engineering aspects:

Sending spoofed e-mails

Building confidence between a phisher and a victim

- Upsetting or exciting statements - must react immediately
- Ask for information such as username, passwords, credit card numbers, social security numbers, etc.
- Emails are typically NOT personalized

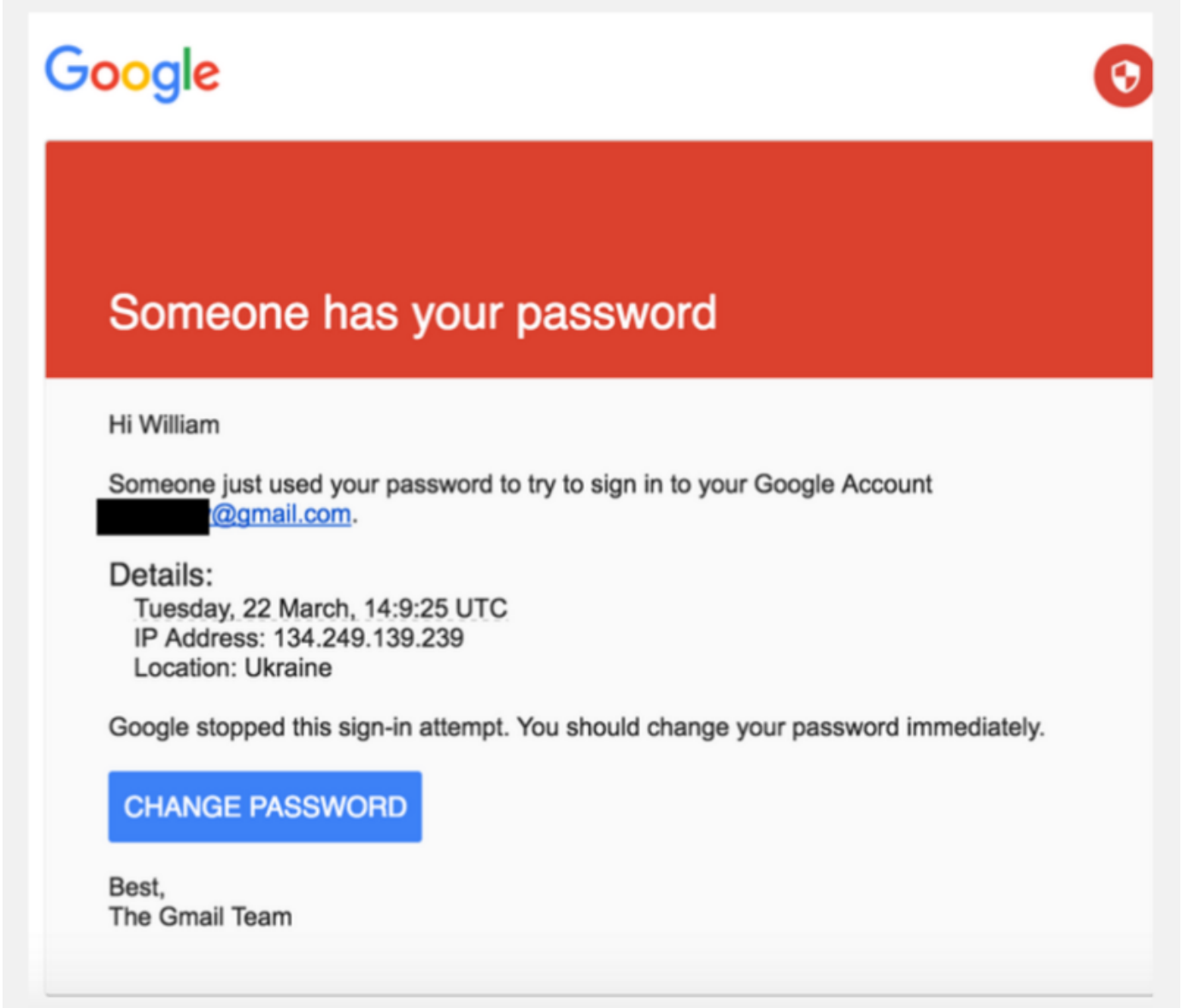
Technical aspects:

Spyware

Pharming - DNS (Domain Name System) poisoning

Spoof web pages

Masked links: e.g., go to
https://www.my.commbank.com.au/netbank/Logon/Logon.aspx, OR
https://www.my.commbank.com.au/netbank/Logon/Logon.aspx



Google

Someone has your password

Hi William

Someone just used your password to try to sign in to your Google Account [redacted]@gmail.com.

Details:
Tuesday, 22 March, 14:9:25 UTC
IP Address: 134.249.139.239
Location: Ukraine

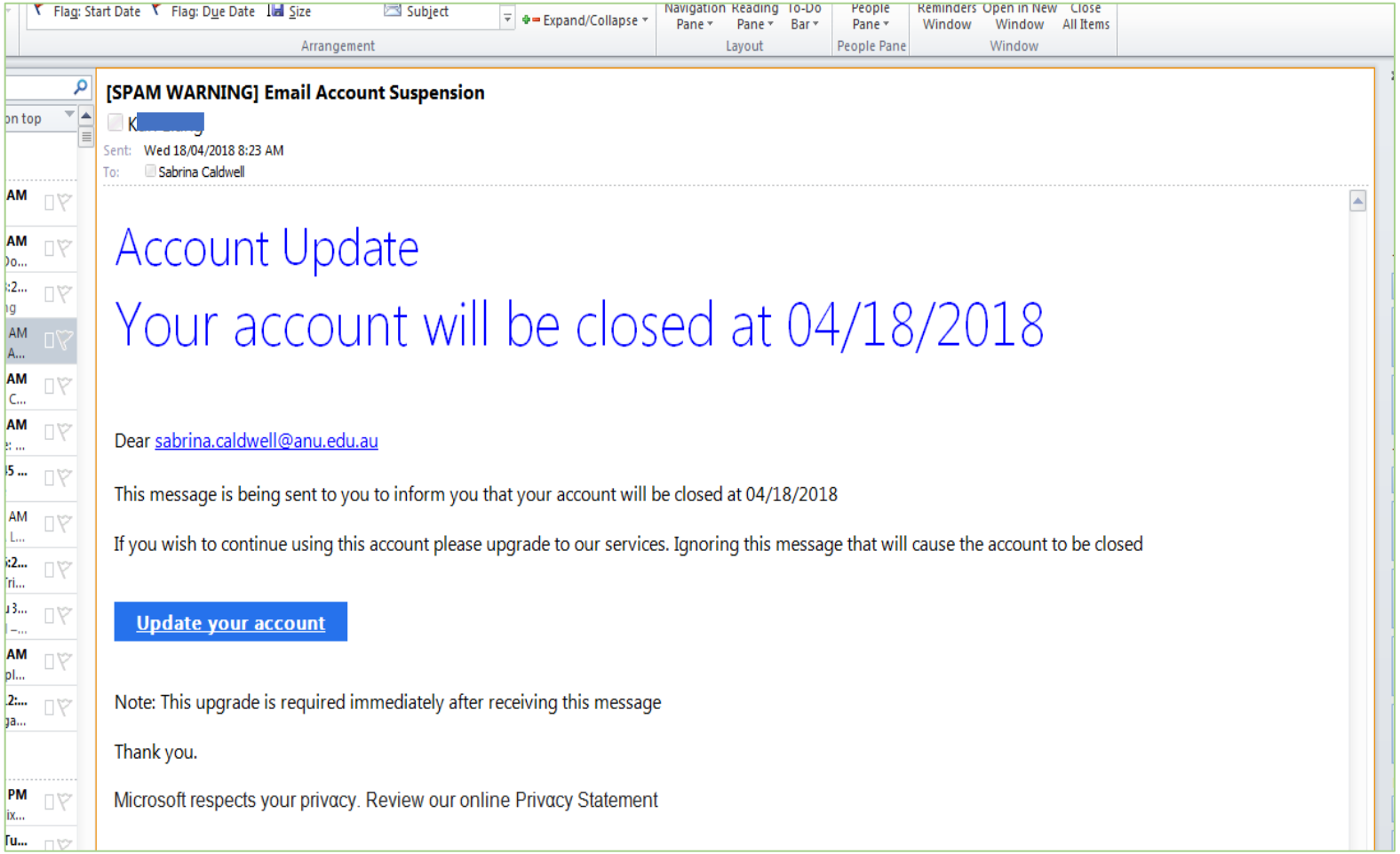
Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

Detecting

- Do you really know who is sending you the email? Do you recognise the sender? Their email address? Is the tone consistent with what you would expect from the sender?
- Are you expecting an email from them?
- Is the content of the email relevant to you?
- Does the email ask you to access a website or open an attachment?
- Is the web address relevant to the content, and accurate?
- Is the email suspiciously written?
- Have you received the same email twice?
- Does the email ask you for your personal details?



Phishing

Phishing is misrepresentation where criminals use social engineering to appear as a trusted identity. They leverage the trust to gain valuable information

- Still a huge problem
- Victim isn't clearly identified (anyone will do!)
  - Users
  - Organisations misrepresented

Results? Identify theft, installation of malware, financial loss, reputation loss

Phishing

Consequences of (successful) Phishing

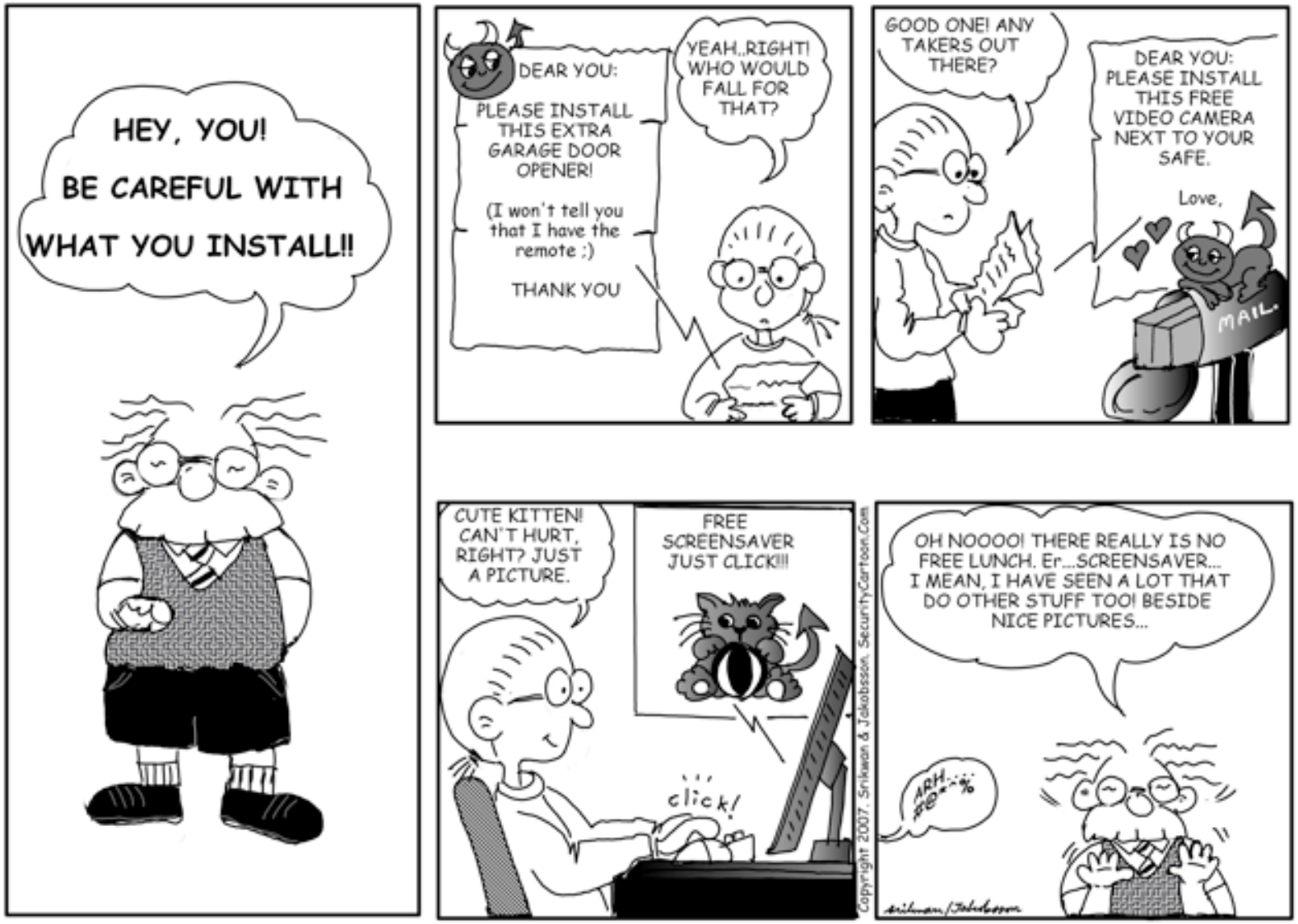
Customers:
Financial consequences ? stolen financial information
Trust and effective communication can suffer

Service providers (banks, retailers...)
Diminishes value of a brand
Customer loss
Could affect stakeholders

Spear Phishing

- Highly sophisticated
- Very targeted at certain people / organisations
- Much more difficult to spot

Example:
Phisher gets an e-mail address of an administrator or colleague
Spoofed e-mail asks employees to log on to a corporate network
A key-logger application records passwords
Phisher can access corporate information!

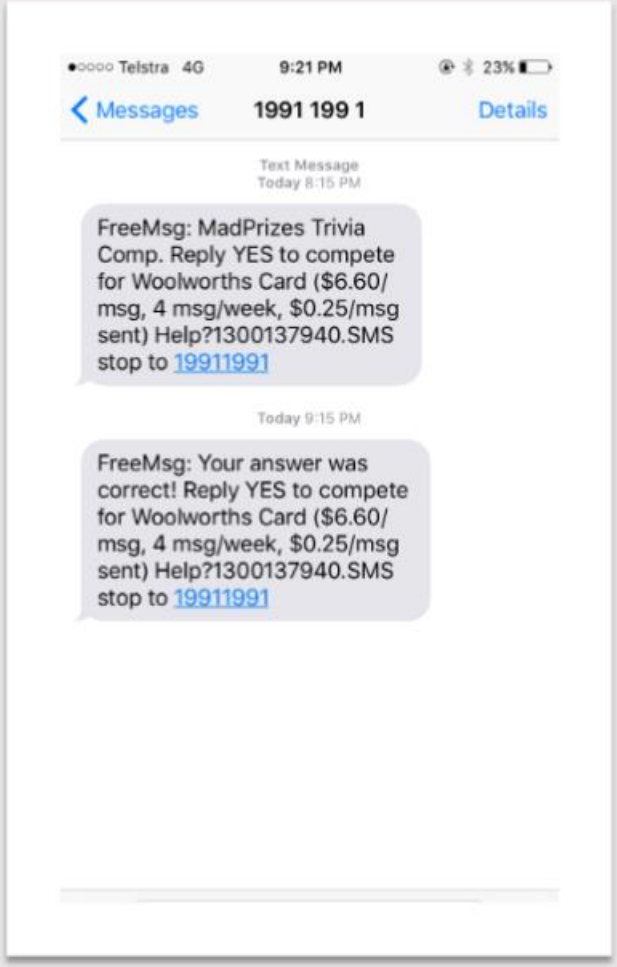


Trusting the Internet Blindly

(Think before you install!)

Mobile phishing

- Real or fake?
- No links or attachments, how much harm could it be?
- What happens if I replied?



Protecting

- Technical controls
  - Attachment filtering
  - Body filtering
  - Domain authentication
  - Sandboxing
  - Whitelisting
  - Etc.
- **User education**

Ideally, all of these in conjunction

Realistically, some combination

Emerging trends

Cyber security is a vast and complicated problem

Many cybercriminals and malicious entities are moving toward social media and instant messaging platforms

Threats are becoming more complex and sophisticated

Always Update

Known security vulnerabilities are patched in security updates

Keep all software up to date

Always use the latest versions when developing

So now what?

‘Rinse and Repeat’

Security landscape is always evolving

Security testing is just one snapshot in time; you must constantly monitor and adapt to new threats

Reporting

Many organisations allow forwarding/attaching of spam emails to their IT Security teams

Individuals can report to the Australian Cybercrime Online Reporting Network (ACORN)

Resources

Open Web Application Security Project (OWASP)

Mozilla Developer Network

W3C Security Resources

Australian Signals Directorate (ASD)
and Australian Cyber Security Centre (ACSC)

A wide variety of security consultancies and organisations and international standards