Click, Click, BOOM

how USC is using Mimecast to overcome click happy user security breaches

Connie McIntosh Manager IT Systems



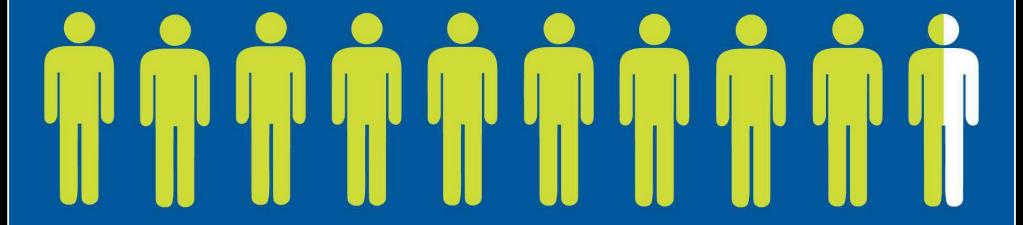
What percentage of successful cyber attacks are caused by human error?

The Human Factor

95%

of all successful cyber attacks is caused by human error

Source: IBM Cyber Security Intelligence Index



The Human Factor

Overview

Background

BEC Statistics

USC Test – Are users click happy?

Mimecast Implementation and challenges

Mimecast Statistics from USC

Questions



USC in 2017 commenced a Cyber Resilience review of IT Systems. Email systems within USC are utilising 0365. It was identified that we needed a complimentary hardening platform to secure the University against the largest attack surface.

Mimecast is one of the largest cloud e-mail security providers and serves over 30,000 organisations globally. Mimecast's "bread and butter" is defending against phishing, ransomware and other targeted e-mail attacks.

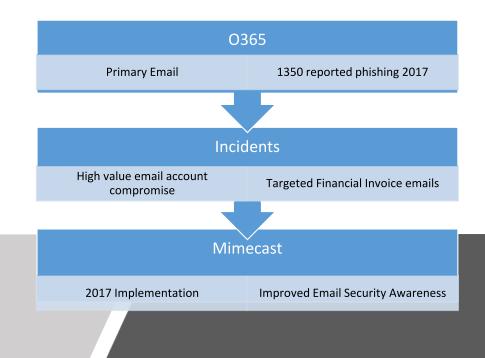
Magic Quadrant

COMPLETENESS OF VISION
Source: Gartner (October 2017)



As of September 2017

@ Gartner, Inc.



Why is email security so important?

Email is still the #1 delivery vehicle for malware

92.4% of malware is delivered via email.

Verizon 2018 DBIR | Tweet this stat

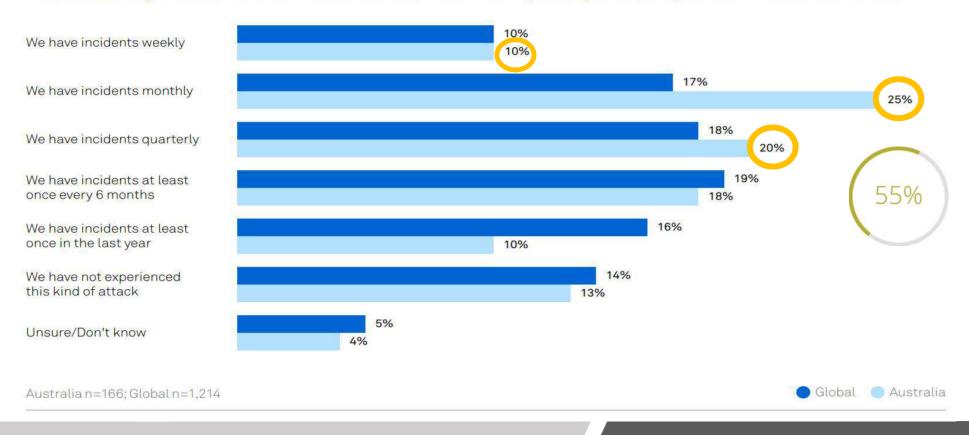
Most popular malware disguises and phishing lures

Fake invoices are the #1 disguise for distributing malware.

Symantec 2018 ISTR | Tweet this stat

Q: How frequently has your organisation experienced phishing attacks in the past year?

A subset of organisations which have had business interrupted by a security breach in last 12 months

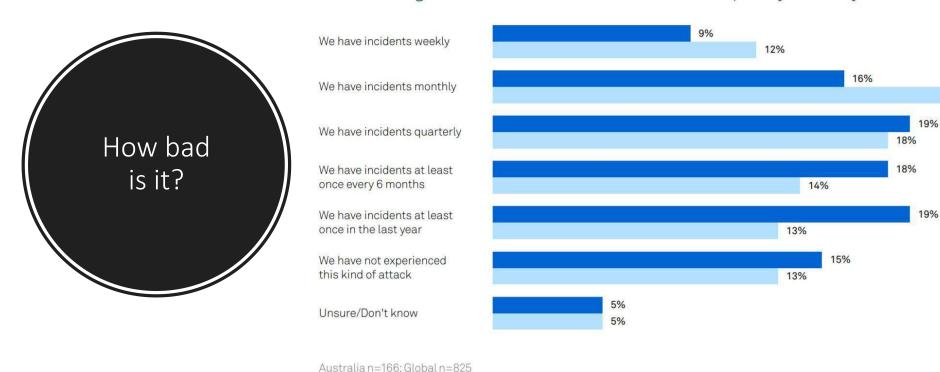


Frequency of Phishing Attacks

Telstra Security Report 2018

Frequency of Business Email Compromise (BEC) Attacks

A subset of organisations which have had business interrupted by a security breach in last 12 months

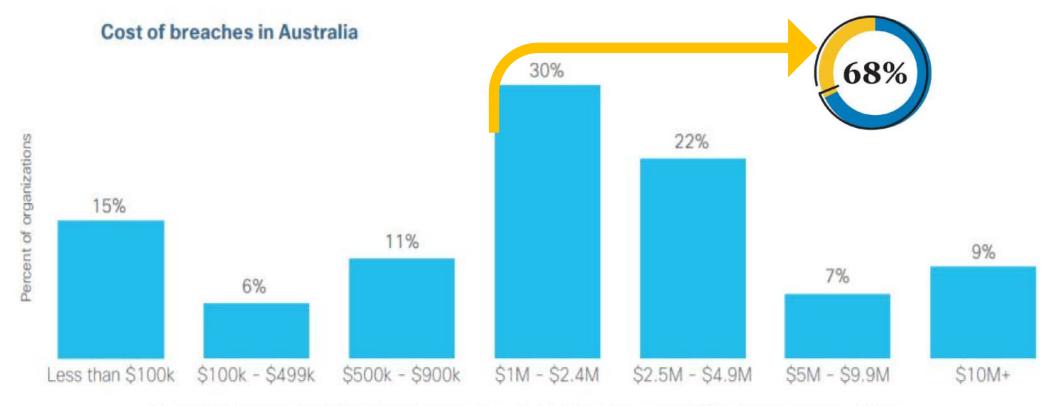


Business Email Compromise Attack Frequency

Telstra Security Report 2018

Global Australia

25%



Q: Thinking back to any attacks in the past year, with all things considered (lost revenue, lost customers, lost opportunities, out-of-pocket costs), what would you estimate the impact of the attack?

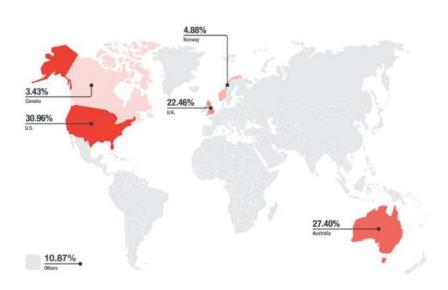
Cost of breaches in Australia

Cisco 2018 Asia Pacific Security Capabilities benchmark Study.



FBI: Business Email Compromise is a \$5 Billion Industry

May 8, 2017 16:21 by Paul



Countries with the most BEC attempts in the first-half of 2017

(Image: Screenshot by Asha McLean/ZDNet)

According to the Federal Bureau of Investigation (FBI), global losses from business email compromise (BEC) since 2013 have reached \$5.3 billion, with a mid-year report from Trend Micro highlighting that CEOs were spoofed the most by BEC attacks.

2018 - Consumer Affairs Victoria has advised real estate agencies to ensure their cyber security is up to date, and home buyers to verify any payment instructions, after receiving reports of more than \$200,000 in losses from an email scams. The email scam works by directly hacking the email accounts of real estate agents.

More than <u>A\$340 million</u> was reported lost by Australian victims of fraud schemes in 2017, up A\$40 million on the previous year.

Iost \$450,000 to BEC
fraudsters after making
nine transfers it believed
were payments to a
professional services
supplier.

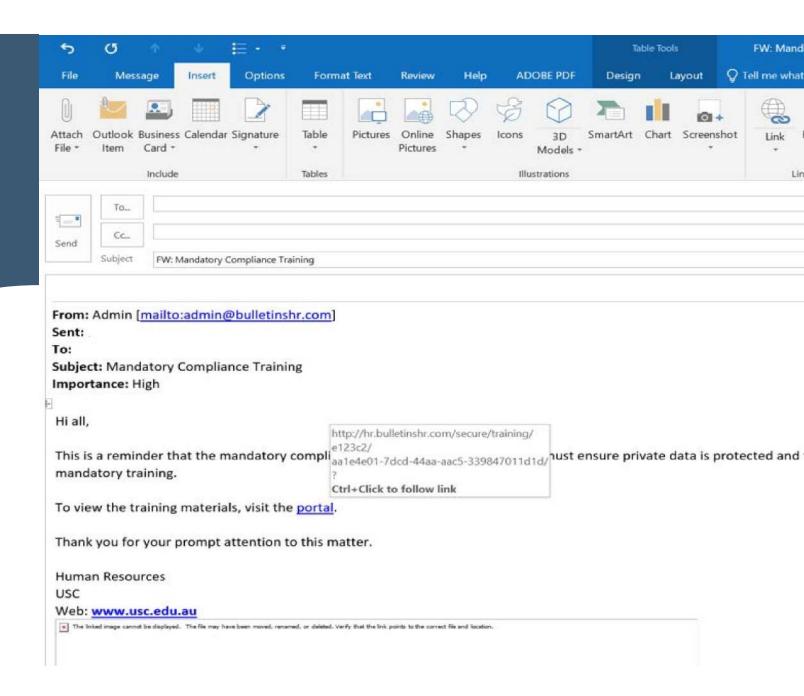
Cost of breaches in Australia

Newspaper sourced

LET'S TEST OUR USERS

I undertook some actual phishing tests to see just how click happy users might be.

Test 1 – Simple email with URL



Are people click happy?

Yes they are...





Test 1 – The first test was designed to be deliberately obvious to see just how click happy people really are



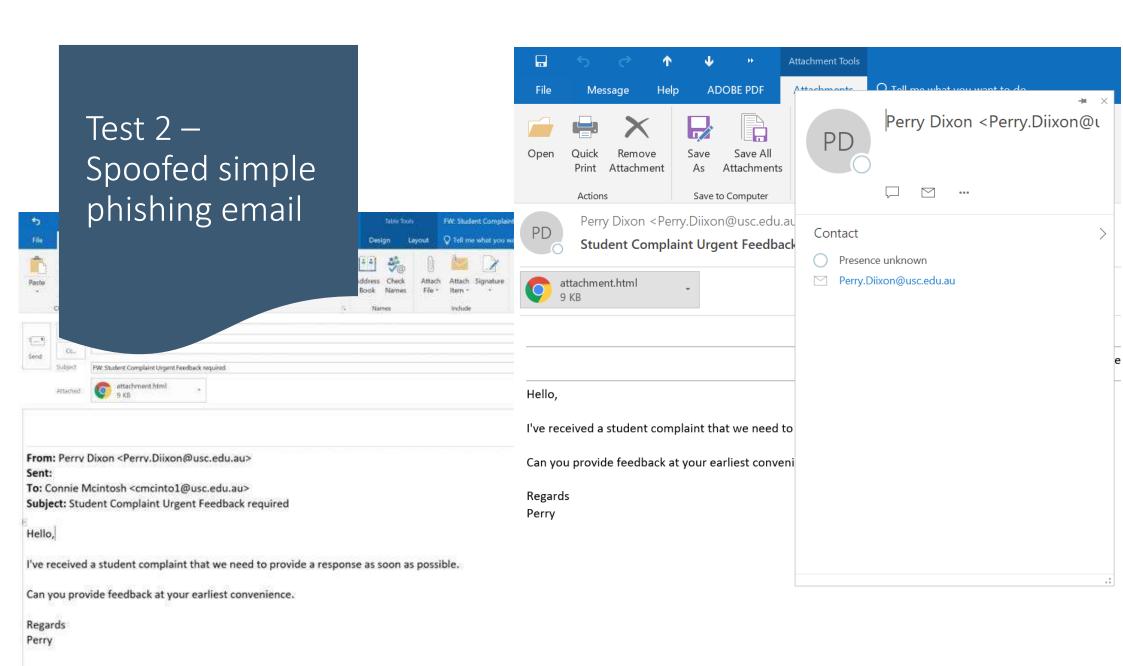
Email from a non USC address with a hyperlink of badness



20% of recipients clicked through to the URL.

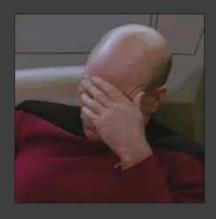


Too Easy



Once bitten twice shy?

Not nearly...





Test 2 – a little more sophisticated, spoofed a real USC user adding an extra letter in the lastname. Test 2 conducted on the same group one week after test 1.



65% click rate



Findings showed >80% of people Who clicked Test 1 also clicked Test 2.

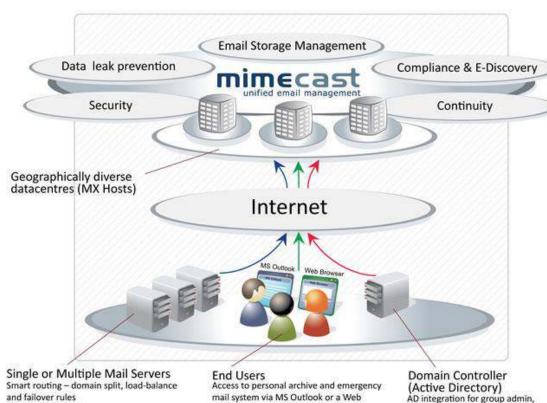


What we know is People WILL click first ask later....

The Mimecast Factor

These tests demonstrated the need to put in place defences against Business Email Compromise.

The Mimecast Factor



Browser

USC chose Mimecast for;

Ease of implementation; and it's ability to provide;

- Reputation
- Blocking dangerous file types
- Blocking or holding encrypted ZIP files or email components
- Spam detection
- Impersonation protection
- URL Protect

recipient validation, authentiation etc

Manual exclusion folders created for Permitted Senders,
 Blocked Senders and Permitted Forwarders





EMAIL ENCRYPTION

STATIONERY MANAGEMENT

DATA LEAK PREVENTION

ANTI-VIRUS \$ ANTI-SPAM

mimecast

COMPLIANCE # eDiscovery

EMAIL FILE ARCHIVE SEARCH

The Mimecast Factor











BOX

SHAPEPOINT

FILE ARCHIVE







JOURNALING



ACTIVE DIRECTORY EXCHANGE

CUSTOMER

IN FRASTRUCTURE











WEBMAIL

MICROSOFT OUTLOOK



The Mimecast Factor

URL Protect & Attachment Analysis

It essentially acts as a URL shortener — similar to bit.ly — and rewrites all inbound e-mail links. When a link is clicked, Mimecast checks the original URL against various threat intelligence platforms and makes a decision whether it is safe for the user to proceed or not.

Attachments are analysed in a cloud sandbox for malware before being sent to the users.



The Mimecast Factor

Impersonation Protection

Real-time protection against malware-less social engineering attacks like whaling, CEO fraud, business email compromise, impersonation or W-2 fraud.



Challenges

The problem is that I can't see the URL in the email itself... just the mimecast nonsense URL. How do I assess if the link is valid or not? Perhaps just click on it and see? That is ridiculous.

Also, this seems like an invasion of privacy of sorts... USC is obviously monitoring and logging every URL that gets send to each person, and also every one that gets clicked on. I should not be forced to browse permanently on "non private" just to accommodate this. (User Education)

I have to type username and password every time I need to access an external link from an email. This is often. (User Education)

#1. User Education

#2 System Configuration

Hi Can you pass on that this new
Mimecast system is annoying. I use a
lot of information feeds and it is time
consuming and unnecessary
Regards
(User Education)

I had a rejected Message" from QUDIT

Unfortunately the header on the panel on the right says "Incoming messages have been blocked by Mimecast for security reasons. No data has been accepted for them and they can't be retrieved." That's personally inconvenient and a cause for worry if it's applying the same rules to other emails for similarly constructed mailing lists that are common across our sector.

(System Configuration)

USC Mimecast Statistics August 2018 1,737,979
Total Inbound Messages
64,072
Weekday Average

292,801
Total Outbound Messages
11,843
Weekday Average

Outbound Malware Detected

Outbound Malware Detected

29,998
Total Clicks
URL Protect

1 in 500

Unsafe Clicks URL Protect



85,442
Total Attachments Sandboxed
Attachment Protect

1 in 2,756
Unsafe Attachments
Attachment Protect

Detections
Impersonation Protect

User Device Pairs Weekday Average





100%

Search Success Rate

Secure Email Gateway

mimecast*

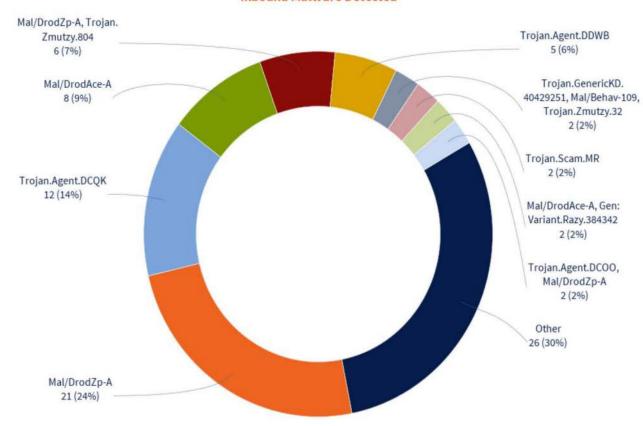


SECURE EMAIL GATEWAYSecure Email Gateway combines strong defenses to keep sensitive information secure.

Inbound Malware Detection August 2018

> The distribution of malware detected in inbound mail. Each instance is counted once per recipient

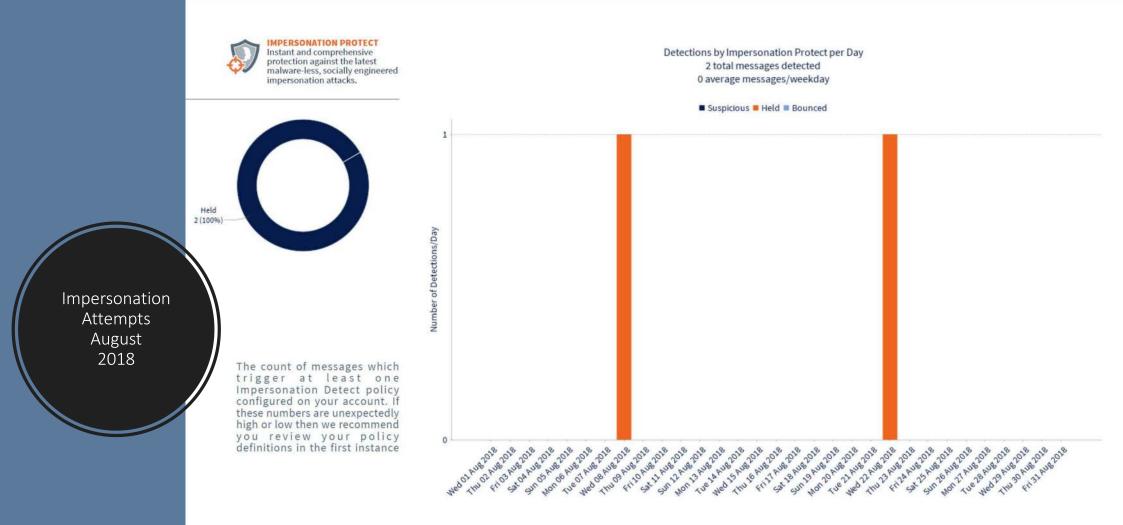
Inbound Malware Detected

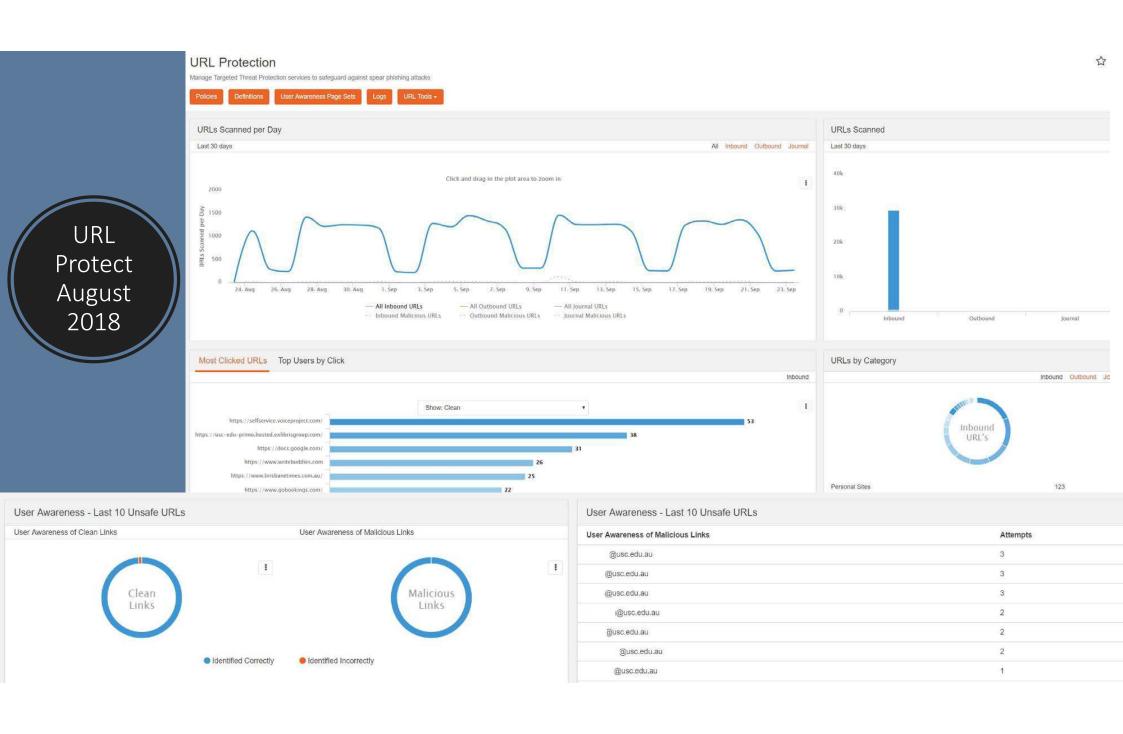


Targeted Threat Protection

Impersonation Protect Detections

mimecast[®]







Thank you

Questions

usc.edu.au usc, quieensland, australia | cricos provider number: 01595D Rise, and shine.