Education & the Human Firewall

How one button, some good marketing and a great team changed Security in TELUS.

Conn Nicoll
Practice Director, TELUS Security

Feb. 10, 2017

To loosely quote Stewart Baker…

Some of the biggest breaches we've seen in the press have come from people who have nothing to do with security.

And from another Cyber Jedi…

> “Half of getting Security right is marketing.”
>
> Marc Kneppers
> TELUS Chief Security Architect

E-mail attacks on the rise

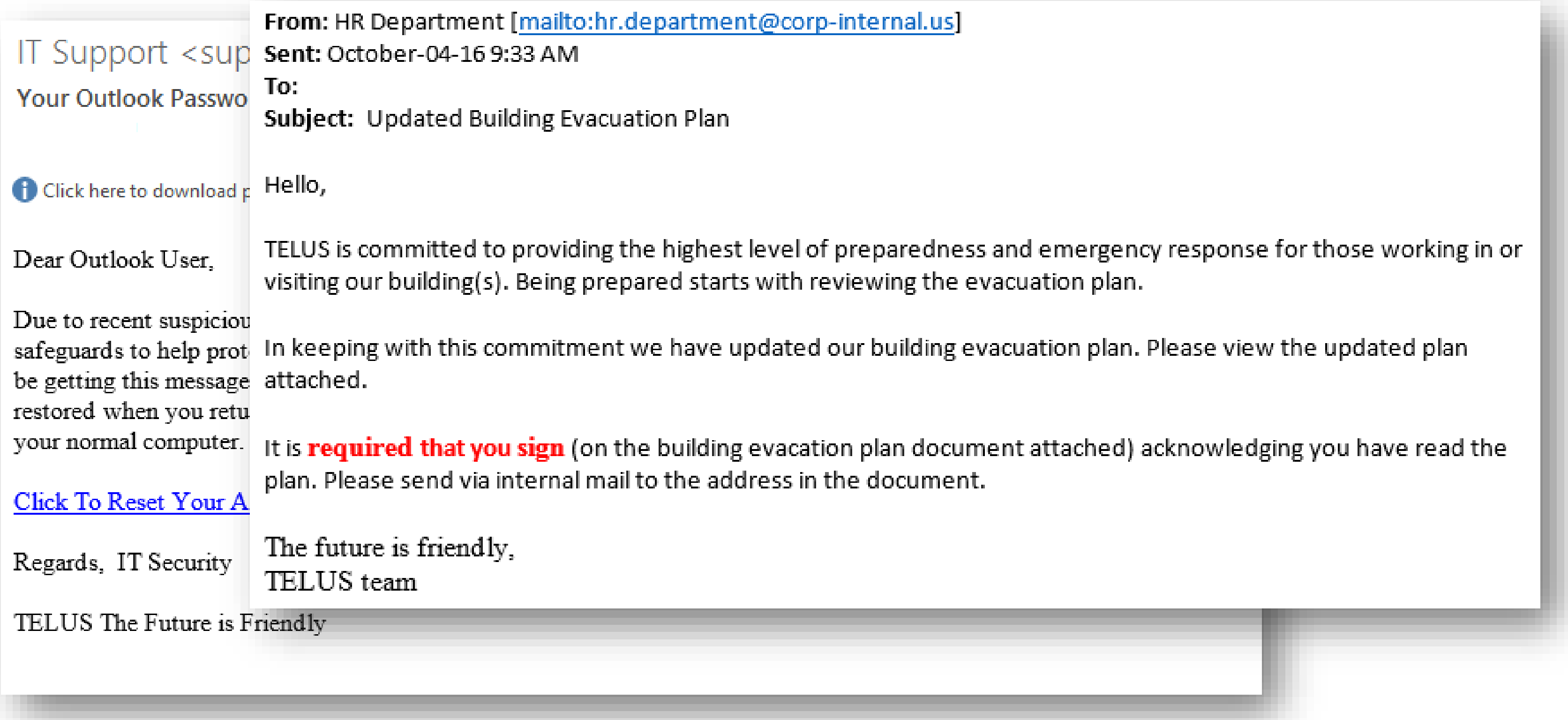
More sophisticated

Better enabled

RSA has stated that 9 of 10 attacks are initiated by phishing

They should know: it cost EMC $66 million to recover from a phishing attack disguised as recruitment plans sent to groups of lower-level employees (2011)

Phishing in Action



IT Support <sup

Your Outlook Passwo

Click here to download p

Dear Outlook User,

Due to recent suspiciou
safeguards to help prot
be getting this message
restored when you retu
your normal computer.

Click To Reset Your A

Regards, IT Security

TELUS The Future is Friendly

From: HR Department [mailto:hr.department@corp-internal.us]
Sent: October-04-16 9:33 AM
To:
Subject: Updated Building Evacuation Plan

Hello,

TELUS is committed to providing the highest level of preparedness and emergency response for those working in or visiting our building(s). Being prepared starts with reviewing the evacuation plan.

In keeping with this commitment we have updated our building evacuation plan. Please view the updated plan attached.

It is **required that you sign** (on the building evacuation plan document attached) acknowledging you have read the plan. Please send via internal mail to the address in the document.

The future is friendly,
TELUS team

TELUS Security Incident Response Team (TSIRT)- Findings

Attack Volume

+176% vs. 2015

Attack type

Malware: 60%

Phishing: 35%

DDoS: 5%

Calculating the Costs

- The immediate cost for a single successful phishing attack including identifying, remediating and blocking further damage from an employee device

$13,282

- Does not include the potential financial impact of any critical data stolen

- Does not include the negative PR and brand damage it can cause to the organization

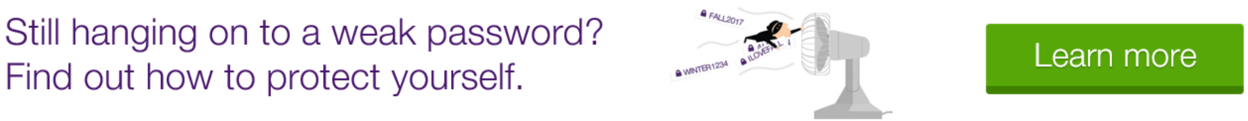
TELUS’ Education Focus

To reduce our exposure, we needed to:

- Convert employees into the first line of defence
- Embed a culture of security across TELUS
- Make employees a part of the detection and response capabilities of our organization

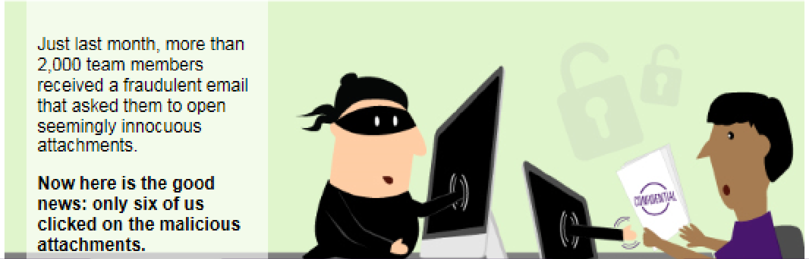
Security Awareness – Spreading the Word

- Leveraging real-world events to educate and engage Team Members
- 5 stories released in 2016 in partnership with corporate communications / TELUS creative



Still hanging on to a weak password?
Find out how to protect yourself.

Received a bogus email about unpaid invoices? Hackers are at play



Just last month, more than 2,000 team members received a fraudulent email that asked them to open seemingly innocuous attachments.

Now here is the good news: only six of us clicked on the malicious attachments.

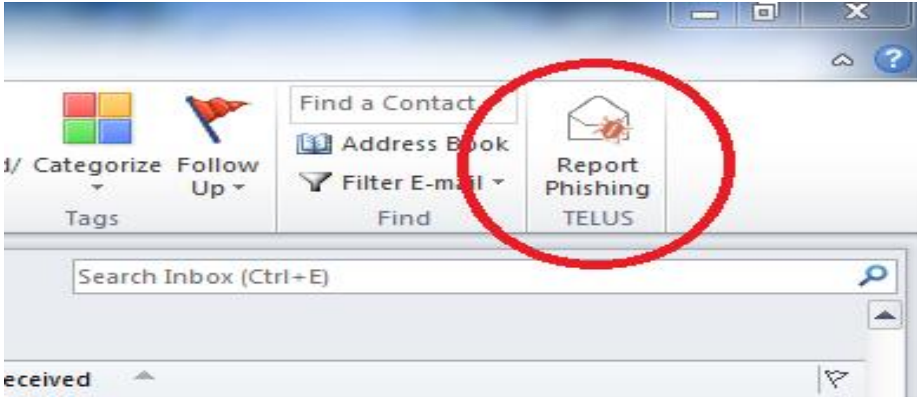
Security Awareness content averaging **1.6x** normal Habitat readership

SPOC - **5x** average password change requests the day of launch

Celebrating wins is now the norm

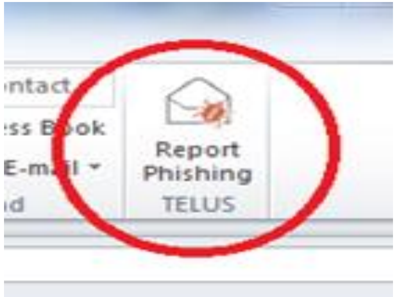
Interacting with TSIRT

Report Phishing button for employees to proactively report suspicious emails



When an employee clicks on the Phishing button, it sets off a chain of events…

Behind the Button: 1



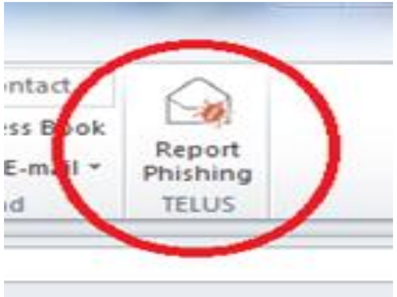
Emails are sent to our TELUS Security Incident Response Team (TSIRT) for investigation and classification as either:

Legitimate

Header info reviewed

- Does reply address match sender?
- Does IP and rDNS address match the email?

Behind the Button: 2



Emails are sent to our TELUS Security Incident Response Team (TSIRT) for investigation and classification as either:

Legitimate

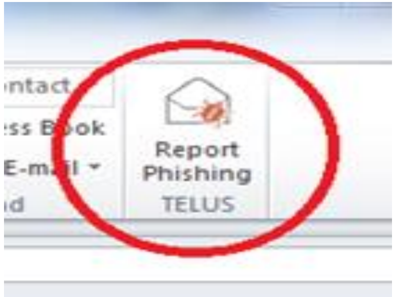
Header info reviewed

- Does reply address match sender?
- Does IP and rDNS address match the email?

Spam

Reply with educational email on the difference between phishing and spam

Behind the Button: 3



Emails are sent to our TELUS Security Incident Response Team (TSIRT) for investigation and classification as either:

Legitimate

Header info reviewed

- Does reply address match sender?
- Does IP and rDNS address match the email?

Spam

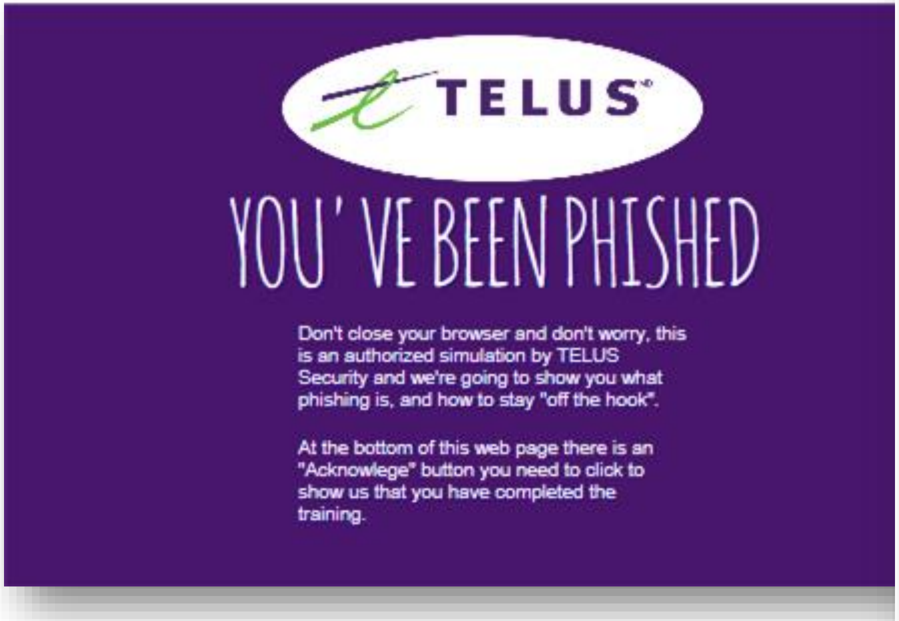
Reply with educational email on the difference between phishing and spam

Phishing

TSIRT examines how many people received email. If enough, future emails from sender and IP are blocked from the network

Is email requesting credentials or does it contain a malicious attachment or link? -> Rule added to firewall to remove attachments

Teachable Moment

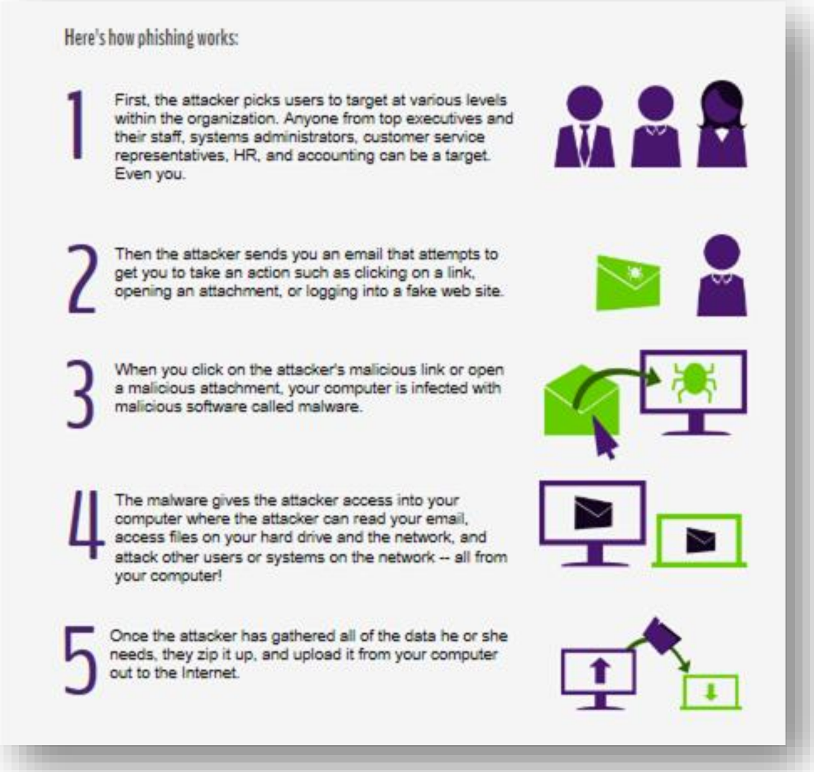


TELUS

YOU'VE BEEN PHISHED

Don't close your browser and don't worry, this is an authorized simulation by TELUS Security and we're going to show you what phishing is, and how to stay "off the hook".

At the bottom of this web page there is an "Acknowlege" button you need to click to show us that you have completed the training.



Here's how phishing works:

1 First, the attacker picks users to target at various levels within the organization. Anyone from top executives and their staff, systems administrators, customer service representatives, HR, and accounting can be a target. Even you.

2 Then the attacker sends you an email that attempts to get you to take an action such as clicking on a link, opening an attachment, or logging into a fake web site.

3 When you click on the attacker's malicious link or open a malicious attachment, your computer is infected with malicious software called malware.

4 The malware gives the attacker access into your computer where the attacker can read your email, access files on your hard drive and the network, and attack other users or systems on the network -- all from your computer!

5 Once the attacker has gathered all of the data he or she needs, they zip it up, and upload it from your computer out to the Internet.

Results

Ongoing education, supported by strong incident response processes and experienced security people resulted in:

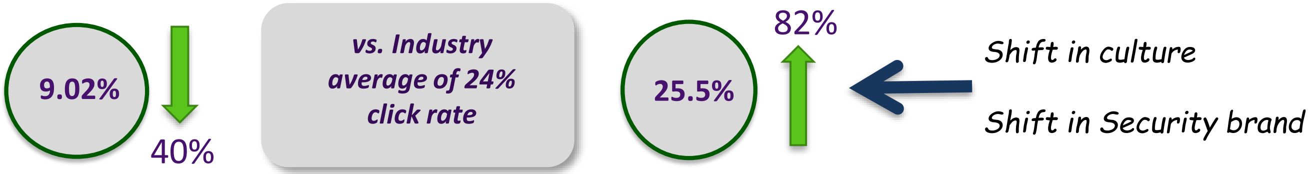
- a significant reduction in clicks on our simulated phishing attacks well below industry averages
- a reduction in successful real world phishing attacks
- a significant increase in the number of malicious emails reported to TSIRT, benefiting the whole organization

Practice makes perfect(ish)

Fake Phishing – AKA Test the Team

Click Rate

Report Rate



9.02%

40%

vs. Industry average of 24% click rate

25.5%

82%

Shift in culture

Shift in Security brand

The Real Deal

Click rate

0.24%

Phishing Attacks

64 incidents

26,676 users targeted

Where to Start

Get the facts…

1. Identify the people with access to your crown jewels.
2. Test their security awareness. The human vulnerability assessment.
3. Compare results against benchmark data and your objectives.
4. Calculate the cost of everyday remediation.
5. Build the plan and the business case. Include internal marketing, process creation and response capability.

Recap

We face a constantly evolving threat landscape. Training and awareness must continue to evolve as to meet these realities.

Our focus will continue to shift towards increased detection and response capabilities – Team Member detection is key.

We will rise and fall based on our collective strength/weakness . We need to engage and enlist all Team Members.

Thank you!

Conn.Nicoll@telus.com

TELUS
the future is friendly®

Building a Culture of Security

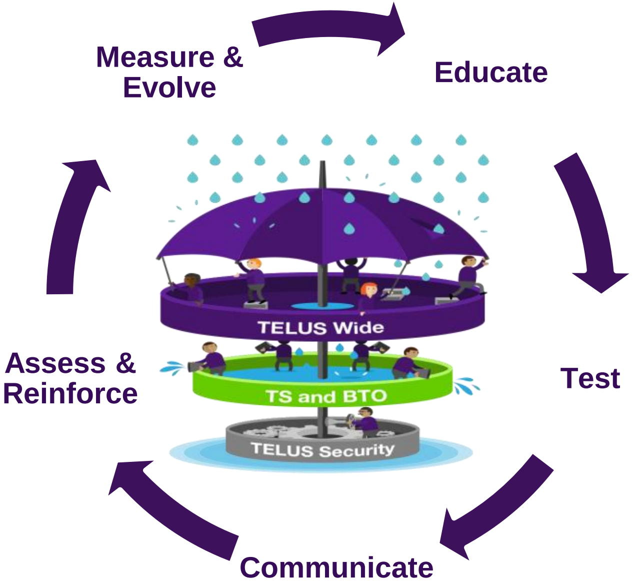
Continuing to build the security community within TELUS

Assessment/testing results reviewed and training evolved to focus on areas of weakness

Supports continued shift to results driven training

Implementing a new platform for assessing Team Member knowledge on specific security topics

Delivering training immediately following assessment depending on result *(2017)*



New, shortened Acceptable Use Policies for Team Members

Improved new hire security course by removing policy language and reduced length by 29%

Over 50,000 phishing simulation emails sent helping to reduce impact of real world attacks

2016 click rate of 9.02% *(well below industry average of 24%)*

5 stories released in 2016 with over 18,000 views

Security awareness content generating 1.5-3x average Habitat readership

Once upon a time…