Phishing Campaign Report
Q3, 2019

جامعة الملك عبدالله
للعلوم والتقنية
King Abdullah University of
Science and Technology

Information Security

Congratulations to our human firewalls for reporting our latest phishing simulation. The fastest in only 9 seconds!

As part of the **Human Firewall Strength Procedure**, to help improve the online security and safety of KAUST personnel, the Information Security department conducts phishing campaigns on an ongoing basis to strengthen the KAUST Human Firewall.

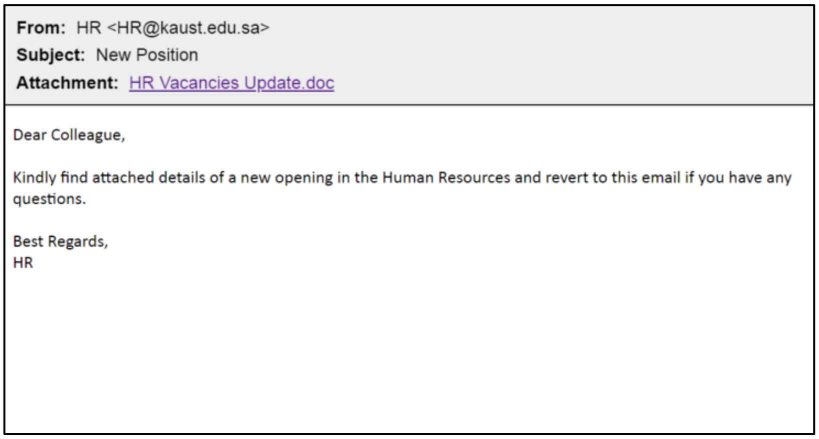
What's New in this scenario:

For the first time since the inception of the Human Firewall program, we warned our community for over a week before the phishing campaign started on screens around campus and by sending an email in advance warning everyone that a phish is coming.

Here's the report for Q3:

A week ago, we carried out an attachment-based spear phishing campaign by sending a phishing email using a kaust.edu.sa address replicating an actual incident that took place at KAUST. The attacker had gained unauthorized access to a kaust.edu.sa account and used this legitimate compromised account to send emails posing as a trusted sender, compelling every recipient to click on malicious links or download infected attachments.

The email we sent was from an email address that exists in the KAUST directory yet is not actively used by HR. The display name was HR and the email address <hr@kaust.edu.sa> which is not the email address that the HR department at KAUST uses to send notifications.



From: HR <HR@kaust.edu.sa>
Subject: New Position
Attachment: HR Vacancies Update.doc

Dear Colleague,

Kindly find attached details of a new opening in the Human Resources and revert to this email if you have any questions.

Best Regards,
HR

Cyber attackers generally target people by using information available online. They often use publicly available information to craft phishing emails and can contact people by different means to catch their attention and trigger emotions to compel them to click and fall for the bait.

We are proud that our community has gained greater social engineering awareness and is able to successfully identify simple and obvious phishing emails.

However, since attacks from trusted sources are a new trend and leading companies like Google and Microsoft are working towards zero trust models; we wanted to assess KAUST's ability to defend against advanced phishing attacks.

You can be rest assured that all security controls around KAUST email systems are in place and fully functional. We had explicit access to spoof (pose as) KAUST email for this phishing campaign only.

We confirm that HR@kaust.edu.sa was not compromised and is a trusted KAUST email address and we appreciate the support and cooperation of the HR department in keeping KAUST secure.

Points to remember:

- Always be sure to re-read emails that seem suspicious and odd.
- Emails sent from a kaust.edu.sa sender are generally valid emails, please don't ignore them.
- Report emails sent from a kaust.edu.sa sender ONLY if the contents of the email seem suspicious.

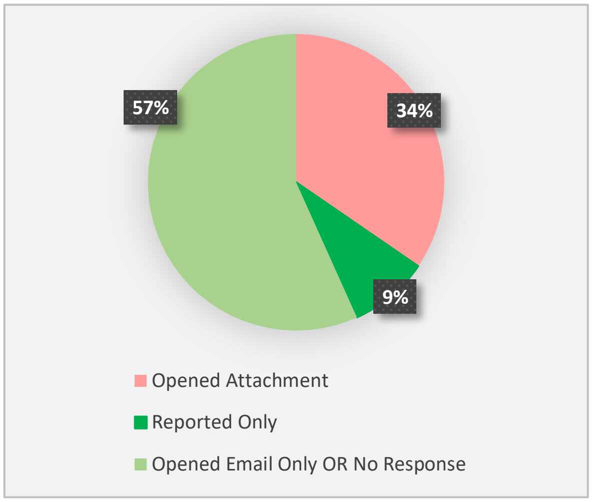
What is Spear Phishing?

Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business by masquerading as a trustworthy entity in an electronic communication.

Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer in attempt to acquire sensitive information such as usernames, passwords, and credit card details and sometimes, indirectly, money.

Response Breakdown:

As the email originated from a kaust.edu.sa address, 34% of recipients opened the attachment.



- In comparison to our previous scenario, we have noticed a 2% decline in the number of people reporting phishing emails.
- 44.9% opened the attachment using a mobile device and 55.1% opened using a computer. Unlike our previous scenario where 58% of users got phished from mobile devices, and 42% from a computer.
- Report rate has increased - 10.42% reported the phish despite opening the attachment unlike our previous scenario where 8.94% reported despite being phished.

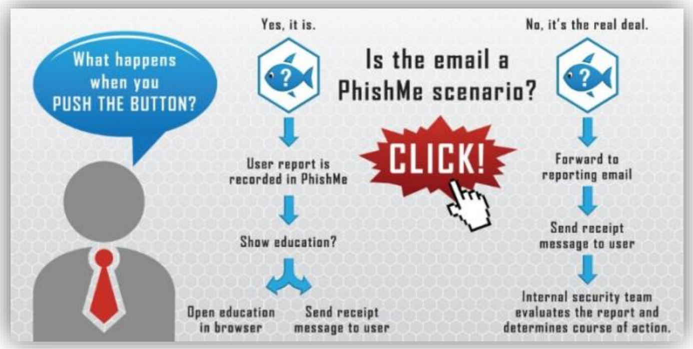
Congratulations to our top reporters!

Fastest Reporters for June 2019	
Winners	Reported within
hussain.sorooji@kaust.edu.sa	9 seconds
clint.harris@kaust.edu.sa	16 seconds
mohammad.shanteer@kaust.edu.sa	20 seconds

Winners, please reach out to us to collect your prizes!

Reporting our phishing simulations and reporting actual phishing emails by using the PhishMe button or by forwarding emails to phishreporter@kaust.edu.sa will help keep KAUST safe from cyber criminals and decrease your human firewall risk score and wins you prizes.

Thank you for being a Human Firewall!


What happens when you PUSH THE BUTTON?
Yes, it is.
Is the email a PhishMe scenario?
No, it's the real deal.
User report is recorded in PhishMe
CLICK!
Forward to reporting email
Show education?
Send receipt message to user
Open education in browser
Send receipt message to user
Internal security team evaluates the report and determines course of action.

For any queries, feel free to reach out to us: askinfosec@kaust.edu.sa

How can you win prizes?

InfoSec carries out simulated phishing campaigns throughout the year to test the human factor. You can win prizes by being 1 of 3 fastest reporters that spot our campaign emails.

Click the ***PhishMe*** button
or
send suspected emails to
PhishReporter@kaust.edu.sa

Click here
for a survey about phishing simulations and redeem 1 point towards your Human Firewall Score!