HACK.LU CFF 2019 / 2019-10-23

FALSE ASSUMPTIONS

OR WHY USER AWARENESS FAILS

SAÂD KADHI

PUBLIC / TLP:WHITE

YET ANOTHER DAY, YET ANOTHER DRIDEX CAMPAIGN

WE SPOTTED A DRIDEX CAMPAIGN

EMAILS WERE DELIVERED TO THEIR FINAL RECIPIENTS

WE WARNED ALL RECIPIENTS: DO NOT OPEN THE EMAILS AND CERTAINLY NOT THE ATTACHMENTS!

(BUT IF YOU DID, GIVE US A CALL)

GUESS WHAT?

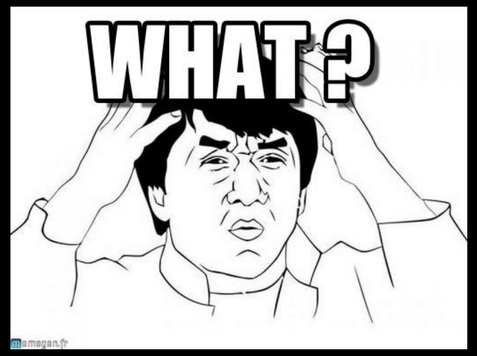
WE GOT A CALL

A USER OPENED THE ‘INVOICE’

THE USER ACTIVATED THE MACRO
BUT COULD NOT SEE THE EXPECTED ‘INVOICE’

THE USER CONTACTED THE SENDER, REQUESTING THE CORRECT INVOICE

(BUT THE SENDER ADDRESS IS FAKE)



‘I’M GLAD YOU WARNED ME BUT…’

THE USER ACTUALLY REQUESTED THAT WE CONTACT THE SENDER AND ASK THEM TO SEND A WORKING ‘INVOICE’

AFTER A GOOD LAUGH, WE DECIDED TO UNDERSTAND WHY

THE USER WORKS IN THE PROCUREMENT DPT.
THEIR JOB IS TO OPEN ATTACHMENTS ALL DAY LONG FROM COMPLETE STRANGERS

THIS IS THE ONLY WAY THEY CAN CHECK IF THE INVOICE CONTAINS A P.O., VERIFY ITS VALIDITY IN THE INTERNAL PROCUREMENT SYSTEM & START PROCESSING IT

CONTINUOUS TUNING OF THE HUMAN IDS

WE SPEND MONEY & TIME, OVER AND OVER

TRYING TO GET USERS TO THINK BEFORE THEY CLICK/OPEN

BUT WE DON'T THINK ABOUT FIXING OUR PROCESSES

OR ABOUT OUR OVER RELIANCE ON EMAIL

AND WE DON'T THINK ABOUT SOME INTERESTING SIDE EFFECTS…

Les Echos

We respect your privacy!

We and our partners use non-sensitive information like cookies or device identifiers for purposes like displaying personalized ads, measuring traffic and preferences of our visitors as well as personnalize content.

Click on the button to consent to these operations and maintain a tailored experience. You can change your preferences at any time by coming back to this website.

View our partners

Don't think. click here

Learn More →

Agree & Close

Pour en savoir plus sur vos droits et nos pratiques en matière de cookies, consultez notre charte cookies.

Le Monde utilise des cookies pour vous offrir une expérience utilisateur de qualité, mesurer l'audience, optimiser les fonctionnalités des réseaux sociaux et vous proposer des publicités personnalisées. En poursuivant votre navigation sur ce site, vous acceptez l'utilisation de cookies dans les conditions prévues par notre politique de confidentialité. En savoir plus et gérer les cookies.

Paramétrer les cookies

Accepter

Don't think. Click here

Ce site utilise des cookies.

En poursuivant votre navigation sur ce site, vous acceptez notre politique de protection des données personnelles et politique cookies, ainsi que le dépôt de cookies et technologies similaires. Nous et nos partenaires traitons ainsi certaines de vos données personnelles, telles que des adresses IP ou des identifiants, afin de réaliser des statistiques visant à évaluer le trafic et l'utilisation des services sur notre site, vous proposer des services, des contenus éditoriaux et des publicités adaptés à vos centres d'intérêt, vous proposer des offres commerciales ciblées en lien avec votre visite sur notre site (reciblage) via différents canaux de communication, et vous permettre de partager des contenus sur les réseaux sociaux. Vous pouvez à tout moment revoir vos choix en utilisant le lien "Modifier mes choix cookies".

Je paramètre

Tout accepter

Nos partenaires

The new European data protection law requires us to inform you of the following before you use our website:

> *We use cookies and other technologies to customize your experience, perform analytics and deliver personalized advertising on our sites, apps and newsletters and across the Internet based on your interests. By clicking "I agree" below, you consent to the use by us and our third-party partners of cookies and data gathered from your use of our platforms. See our Privacy Policy and Third Party Partners to learn more about the use of data and your rights. You also agree to our Terms of Service.*

☐ I agree

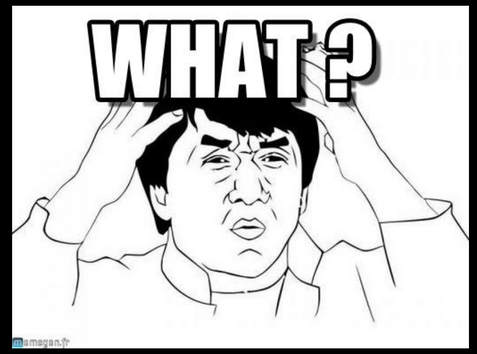
Continue to site

Cookie consent

Patagonia requests that you consent to the use of cookies, JavaScript and HTML 5 and other digital technologies ("cookies") on this website to collect information from your device. These cookies are used to operate the website, measure website audience, provide social media functionality and enable (behavioral) advertising. Social media- and advertising cookies are provided by third parties. Your click on "Agree and Proceed" will indicate to us that you consent to the placement of these cookies on your device in accordance with our cookie notice and to the processing of the personal data that is obtained by means of these cookies. If you wish to change your consent, please click "Adjust Preferences" and adjust your preferences per cookie category. Each cookie category is described in more detail in our cookie notice. Collected personal data will be processed in accordance with our privacy notice.

Agree and Proceed

ON ONE HAND WE TRAIN USERS TO THINK BEFORE THEY CLICK/OPEN



ON THE OTHER HAND, WE TRAIN USERS TO CLICK WITHOUT THINKING

(TO GET RID OF THOSE ANNOYING BANNERS)

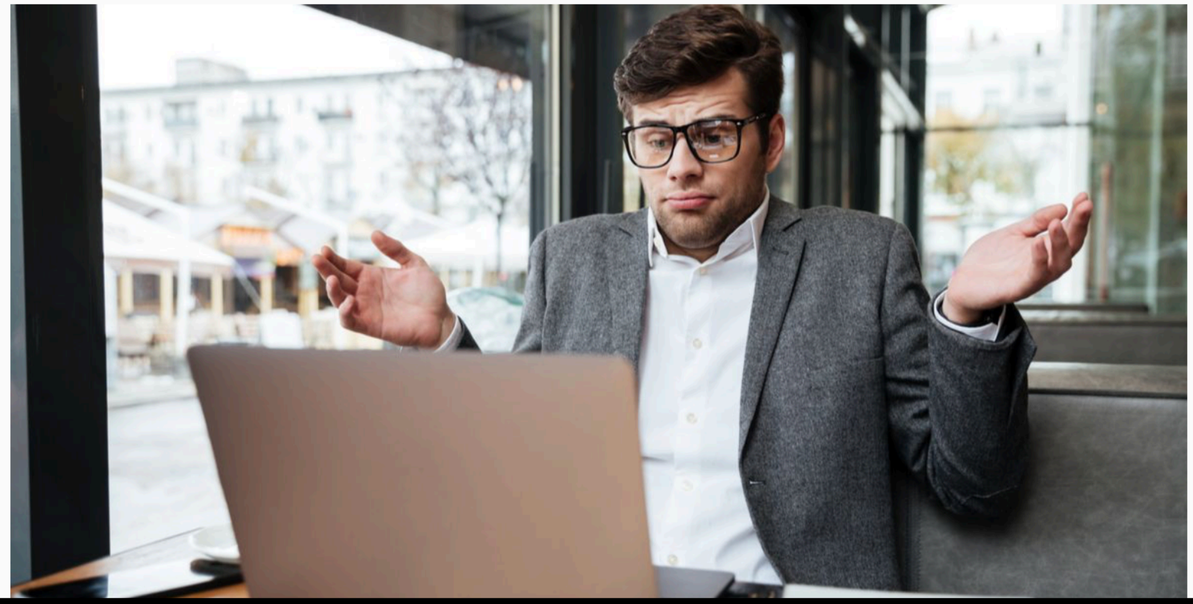
ARE WE TRYING TO DRIVE THEM MAD?

Source: Naked Security

Most Americans don't have a clue what https:// means

11 OCT 2019 8

2-factor Authentication, Security threats



AND THEY SHOULDN'T CARE!