aimbrain
simply smarter authentication

Newsletter

JANUARY 2019

MUST READS THIS MONTH

Epic Games' bug infestation leaves Fortnite accounts vulnerable to hacking
(Dark Reading)
READ MORE

Biometrics not just for consumers as Citi Treasury and Trade trials corporate use case
(Finextra)
READ MORE

Mobile banking gets overtaken by banking apps as consumer channel of choice
(Finextra)
READ MORE

iloveyou qwerty: 2018's worst passwords are out and (spoiler alert) - they're still terrible
(TeamsID)
READ MORE

Reddit got stuffed - credentially
(SC Magazine)
READ MORE

XSS up, IoT down; a rundown of the web app vulnerability trends in 2018
(Imperva)
READ MORE

Gone phishing: credential compromise via phishing attacks up by more than 70% YOY
(Dark Reading)
READ MORE

MUST READS THIS MONTH

Andrius Sutas, CEO, AimBrain
Breach headlines suffer from sensationalism too

"Most of us won't have missed the megabreach headlines, where 87GB of personal data, including 773m unique email addresses and nearly 22m passwords, were found on a MEGA cloud server. Before you run for the hills, **check out Krebs On Security's post that painted the real picture**. Most of the data was at least two to three years old, and dubbed by Have I Been Pwned's Troy Hunt as "made up of many different individual data breaches from literally thousands of different sources." What we should be concerned about is the 4TB of data, allegedly less than a year old, that the hacker claims to have for sale. Breaches will continue to happen, so it's not just the technology that needs to change, but consumer attitudes to security. Reusing passwords or continuing to use disturbingly weak ones (see above Must Reads) makes you vulnerable. We're pleased to see organisations addressing this through biometrics - behavioural analytics and anomaly detection for example - but more must be done to educate users about the risks too."third party specialists, often via open APIs, there really is no excuse for not addressing vulnerabilities."

NEWS & MORE

Security tip of the month

As mentioned in the Reddit story above, 2018 saw more and more credential stuffing; where fraudsters took breached passwords and tried them across loads of different sites, aiming to get lucky on some. Never reuse passwords, even if you think that you've got a failsafe way of making them slightly different based on the site. If you must use passwords without two-factor authentication or biometric security, make sure that you use a password generator to create one that is unique and random.

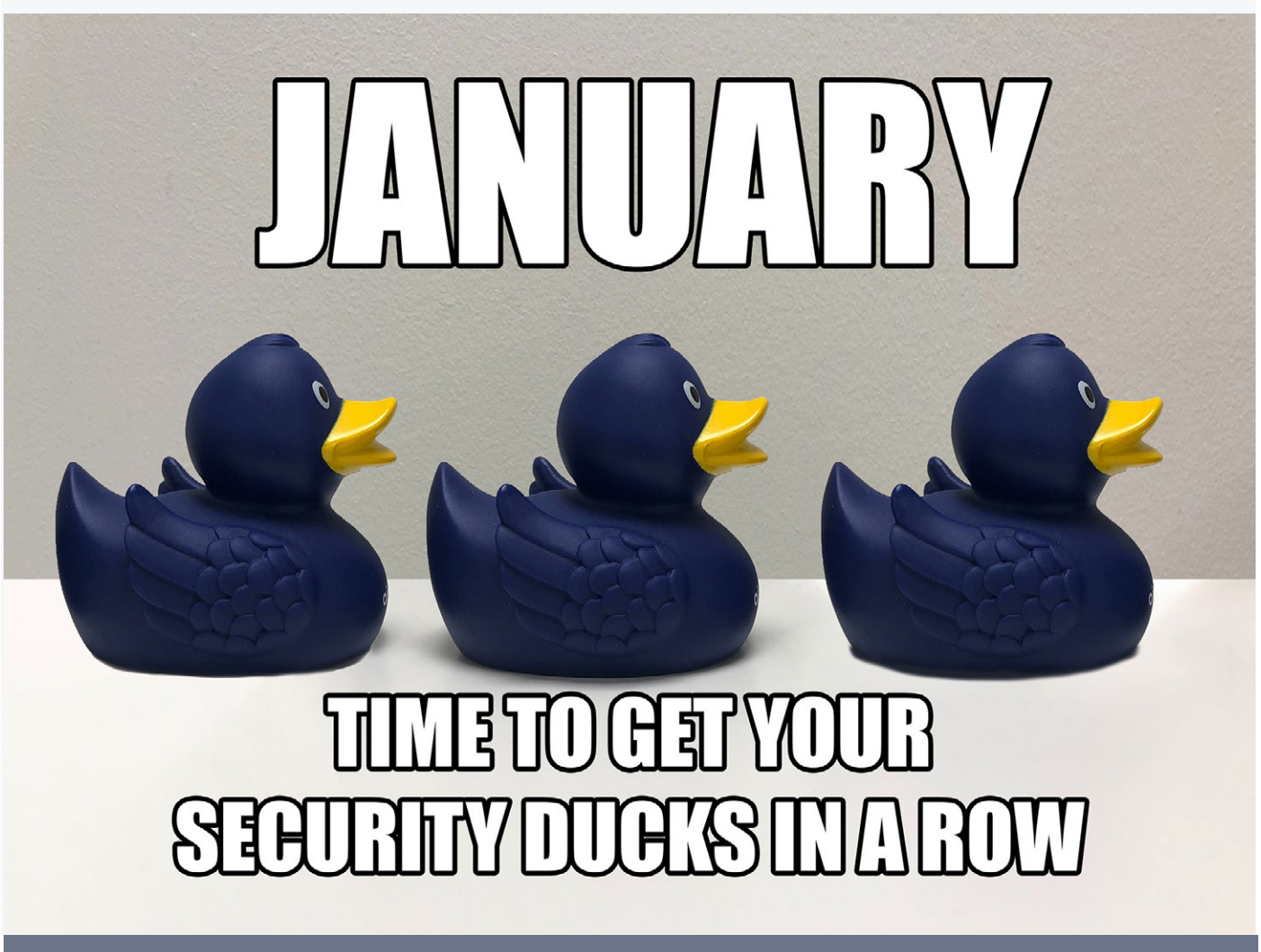
.....

Company Update

Join us for one of our presentations: **Biometrics Institute** (Feb 15, London), PCI Pal and the **Future of Payments and Compliance** event (Feb 21, London) and **ForgeRock Identity Tech Talk** (Feb 26, London). We'll also be at the launch of the **EPA's whitepaper on Financial Crime** (Jan 31), which we contributed to.

And finally, if you haven't already read our CEO interview with Computer Weekly's Karl Flinders, **check it out here.**

.....



MEET THE BRAINS BEHIND THE BIOMETRICS

Will Miller, Business Development Manager, AimBrain

If I wasn't Business Development Manager I'd...
...be running a brewery, or at least being a professional beer taster.

Best quality
My simultaneous inability and enthusiasm for cooking.

Worst habit
Going on about Yorkshire.

I couldn't live without...
...my new, but very old, Ford Focus Estate 1.8.

AimBrain, Level39, One Canada Square, Canary Wharf, London, E14 5AB, UK