IDEE

Alex Christophe
Vertriebsleiter bei IDEE GmbH
Hamburg
alex@getidee.de

Keywords: Building, Enduro, Red Wine, Curry, Ford, Humour.

VAPS - IDEE - MSFT

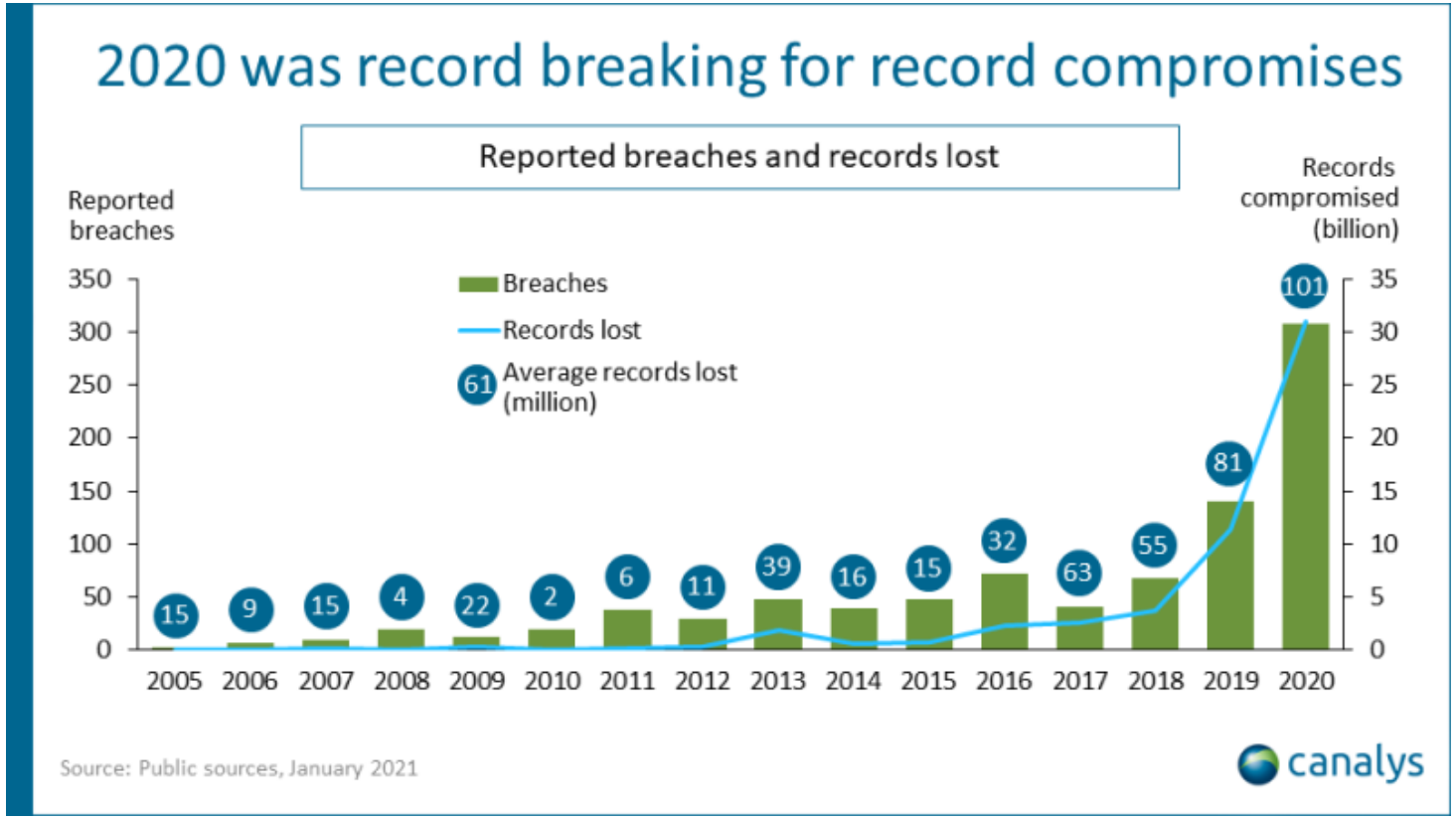
Besser Zusammen

Egal was passiert, Verstöße und Ransomware nehmen zu.

Und egal was getan wird, der Trend sieht nicht gut aus.

Wichtige Veränderungen im 21. Jahrhundert:

'04 NIST: Passwörter alle 90 Tage ändern
'10 Google: 2FA ist für alle verfügbar
'17 NIST: Passwörter nicht regelmäßig ändern
'20 WEF: 80% aller Angriffe sind passwortbezogen
'21 Verizon: 84 % der Verstöße betreffen Anmeldeinformationen
'22 Munich Re: 90% aller Sicherheitsverletzungen beginnen mit Phishing



Mehr Datenschutzverletzungen im Jahr 2020 als in den vorangegangenen 15 Jahren trotz eines Anstiegs der Cybersicherheitsausgaben um 10 %.

MFA ist eine Voraussetzung.

Aber, die Bereitstellung von MFA ist eine Herausforderung

IT-SA-Umfrage – Hindernisse für MFA

Die Gründe, warum Unternehmen MFA nicht **für alle Benutzer** bereitstellen können, sind fast jedes Mal identisch.

Kein 2. Gerät

Unternehmen wollen nicht die Kosten und die Logistik, jedem Mitarbeiter ein 2. Gerät zur Verfügung zu stellen

Keine Zeit

Eine „normale“ MFA-Bereitstellung erfordert Zeit und viele Überlegungen zur Ausnahmebehandlung: Push, SMS, Anruf, nichts

Kein Personal

IT-Abteilungen haben nicht genügend Ressourcen.

Eine Möglichkeit ist, einen MSP wie die VASP zu nutzen.

Kein Investment

Was mit einer "kostenlosen" Basis-MFA-App beginnt, wird sehr schnell teuer, da zusätzliche Lizenzen erforderlich sind.

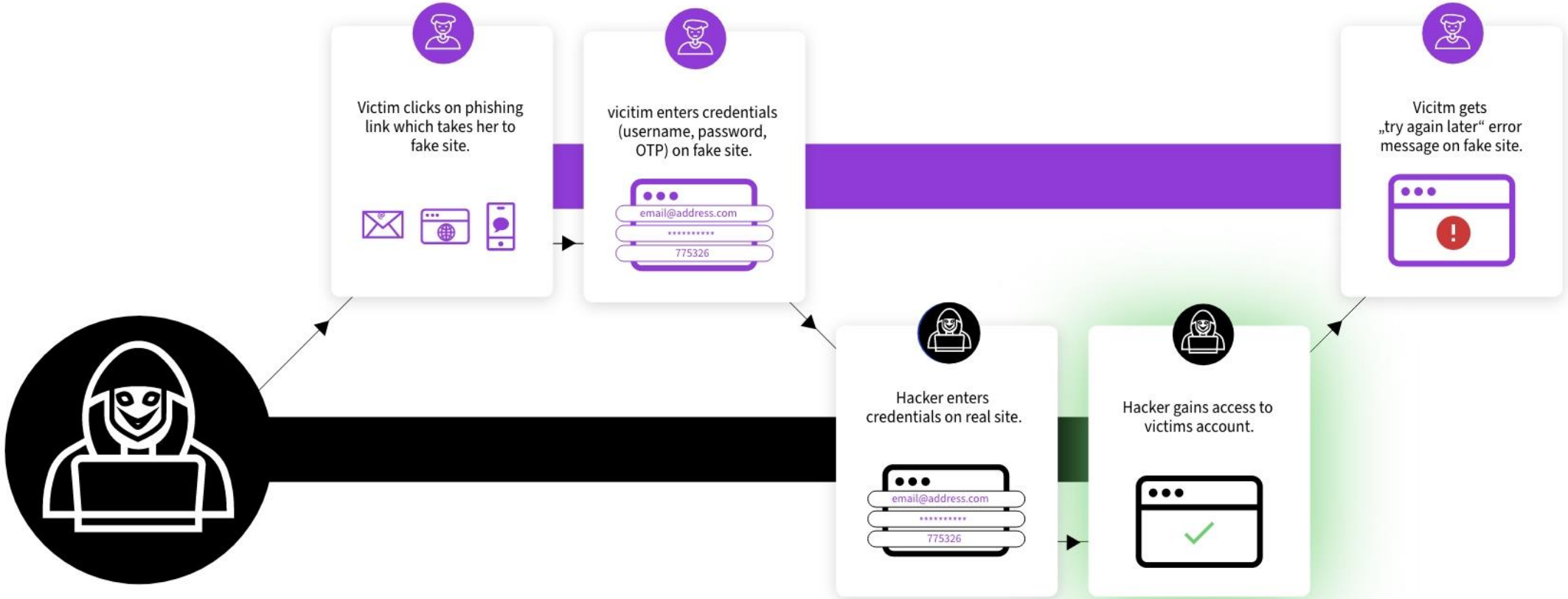
Kein Phishing-Schutz

MFA wurde nie entwickelt, um Phishing zu **stoppen.**

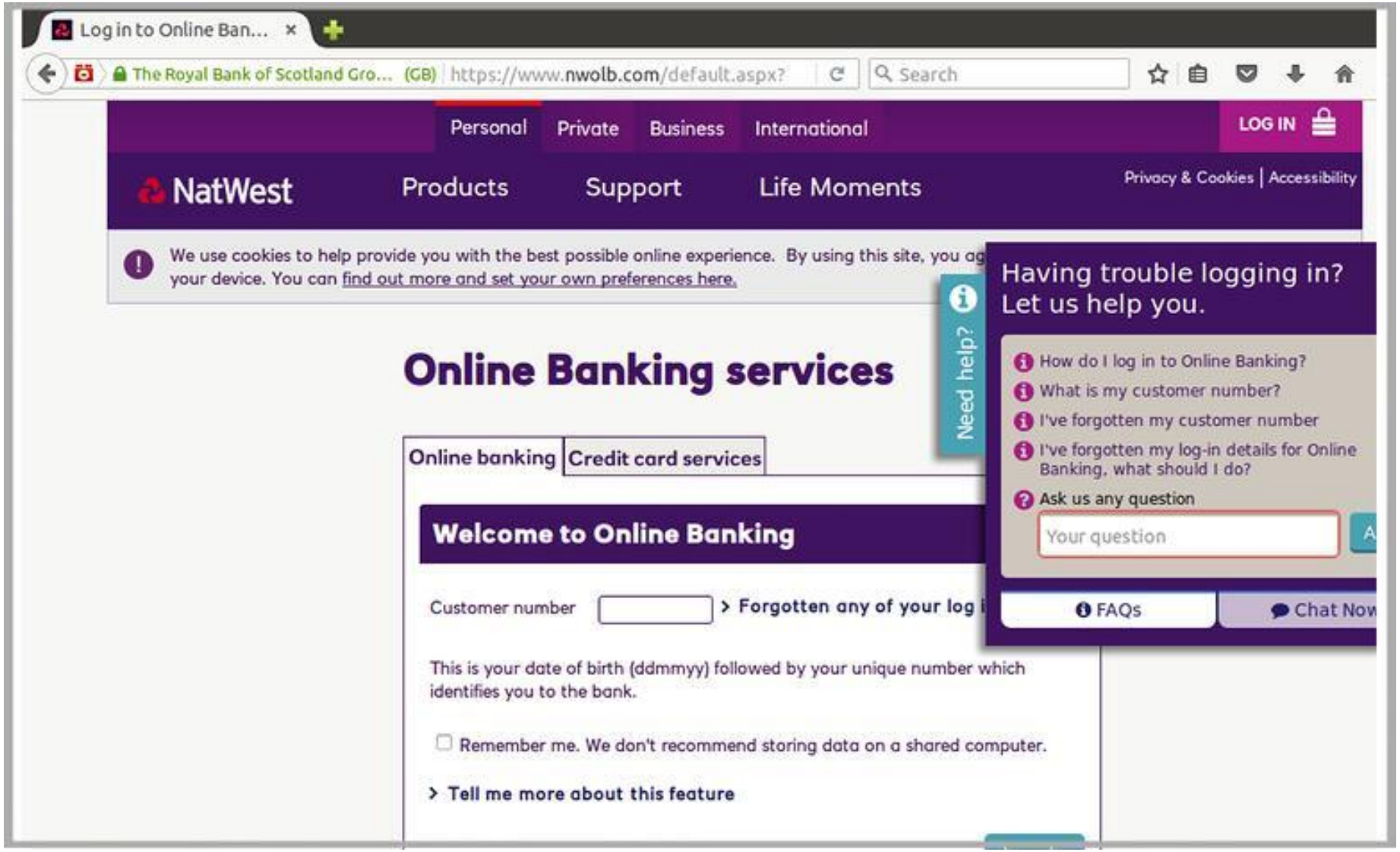
Und das kann es auch **nicht**.

Können Sie es erraten?

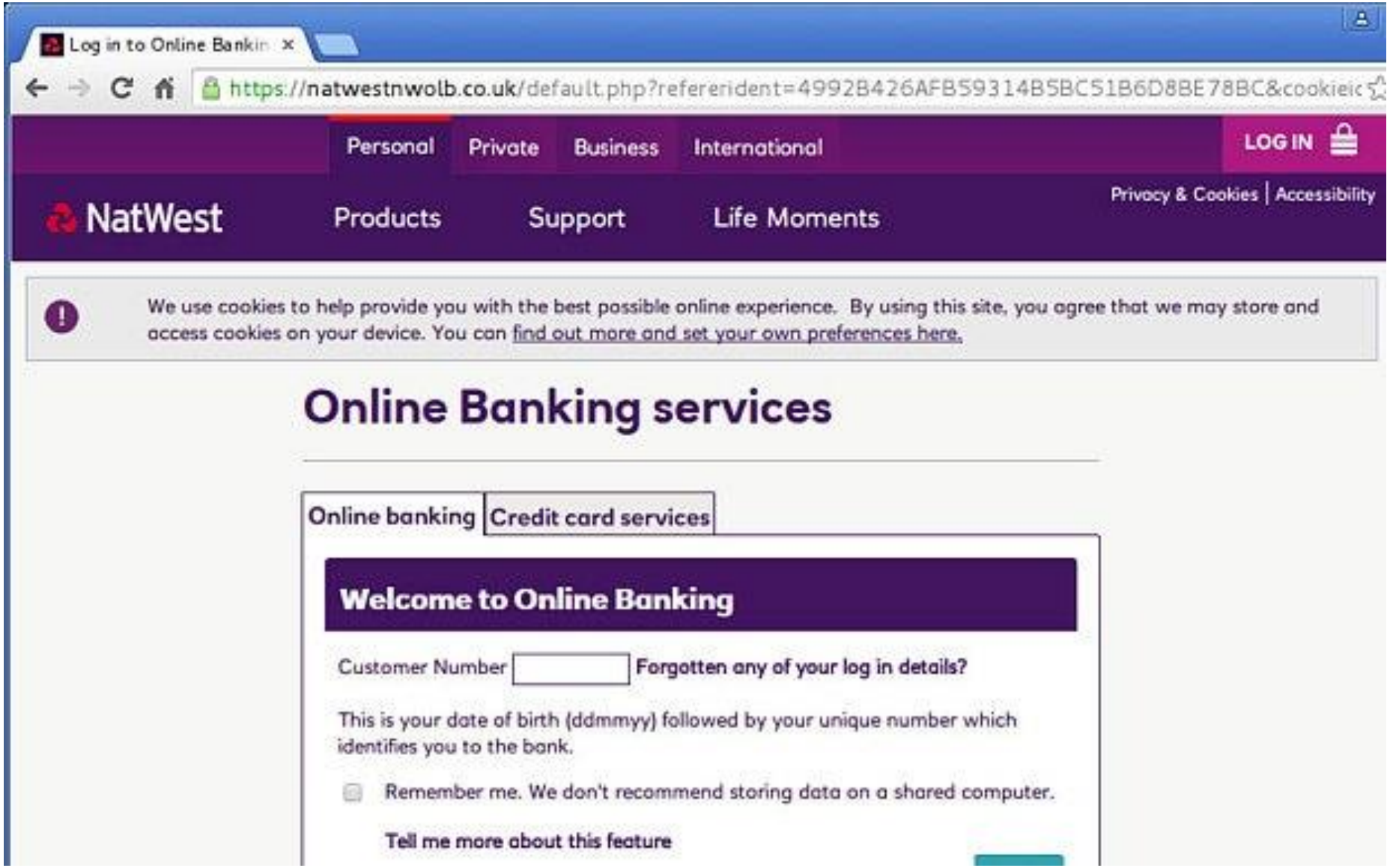
Wie wird Credentials-basiertes MFA gephisht?



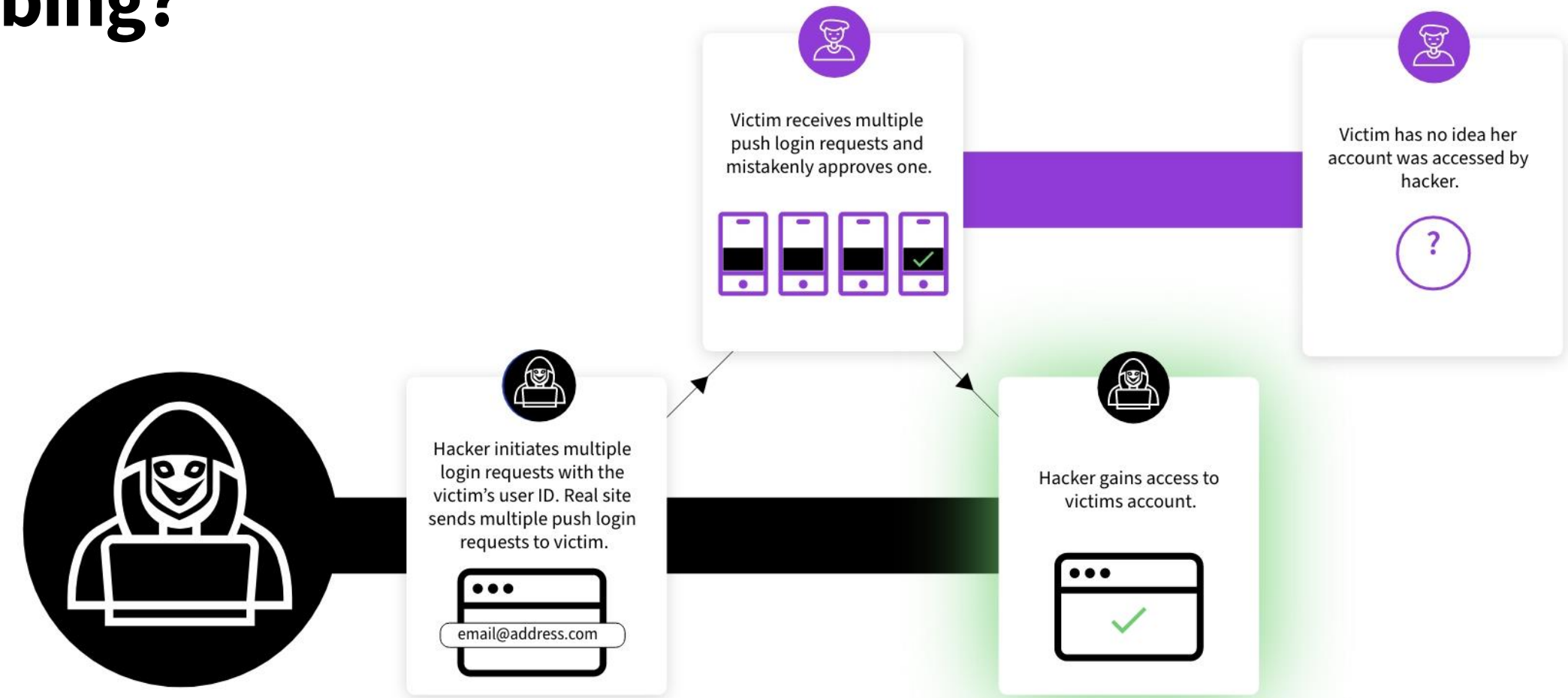
Gefälscht oder legitim?



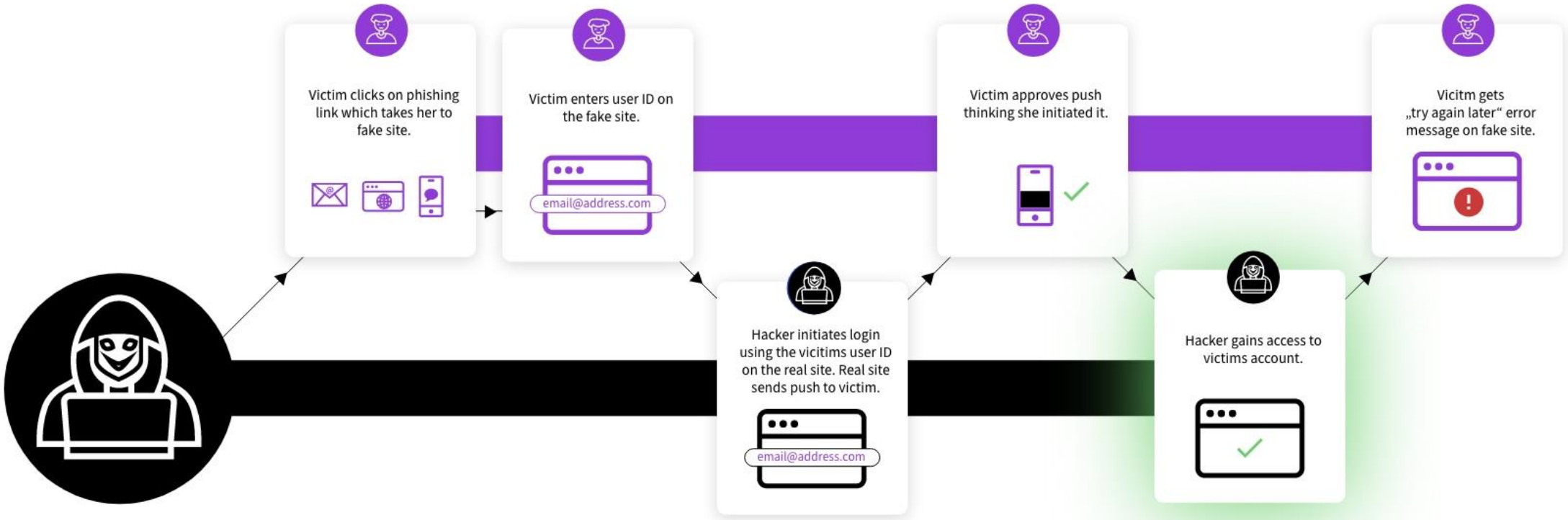
Gefälscht oder legitim?



Wie funktioniert Phishing über Prompt Bombing?



Wie wird Push-basiertes MFA gephisht?



Authenticator MFA Hack Demo

Authenticators (alle!) sind kleine Tore

MFA

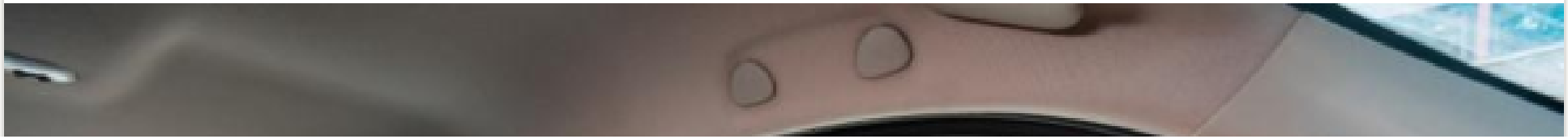
Eine Methode mit mehr als einem Authentifizierungs-faktor.

<u>MFA ist kein Ergebnis!</u>

Deswegen, die Rolle von mehr Kontrollen durch risk-based oder conditional access für Legacy oder 1st Generation MFA ist entscheidend.

Alexandre BLANC Cyber Security (He/Him) • 1st
vCISO - ISO/IEC 27001 and 27701 Lead Implementer - best Cyber Risk Com...
1w •

"The Uber Breach: A Time-Tested Recipe For Disaster"
An interesting take on how, and a way to bring solutions. Yet, many options are possible to fix the issue, one being stop trusting the cloud and enabling conditional access everywhere.
Fun fact is that this is a native feature of most cloud solutions, it's just not enabled.
Then we'll be able to look at the invasive cloud itself, and see if there is any solution to protect our data from nosy cloud provider that won't hesitate to read, mine and exploit data that is not theirs.
connected=hacked
#cybersecurity #cloud #data



AuthN by IDEE

Das sicherste **MFA** auf dem Markt.

Es verhindert jeden einzelnen Phishing- und passwortbasierten Angriff.

Made in Germany

Security by Design

Privacy by Design

100% Phish-Sicher

Ohne 2. Gerät oder Softwareinstallation

Bereitstellung in Minuten

Für die Belegschaft

Für die Lieferanten

Für die Partner

Für die Kunden

Für IoT-Geräte

MFA. Phishing-sicher.
Nur mit Ihrem Gerät.

AiTM Angriffe sind mit AuthN nicht erfolgreich

IDEE

VAPS

Bitte besprechen Sie die Details und Anforderungen Ihrer Projekte mit unserem Partner der VAPS GmbH

Multi-Faktor-Authentifizierung Next-Generation (MFA-NG) Powered by IDEE

oder fordern Sie einen Rückruf über unsere Website an, indem Sie diesen QR-Code scannen.

SCAN ME

Security by Design

Privacy by Design

Made in Germany

VAPS - IDEE - MSFT & Co. - Partnerschaft