DLRG
Landesverband Württemberg e.V.

Die Auswertung Ihrer sicher3 Phishing-Kampagne

Was ist Phishing?

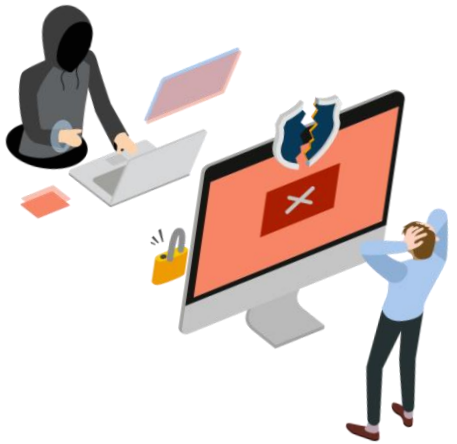
„Eine skalierbare **Täuschungshandlung**, bei der eine **falsche Identität** benutzt wird, um **Informationen** von einer Zielperson zu erhalten, oder sie zu einer von ihr **ungewollten Handlung** zu bewegen."

…bekannt seit den frühen 90ern

…bekannteste Form des Social Engineering

z.B. Namen, E-Mail-Adresse etc.

z.B. Benutzerdaten eingeben, Geld überweisen



Statistiken zur Cyberkriminalität

Cybercrime-Bilanz: 7 von 10 Internetnutzern betroffen

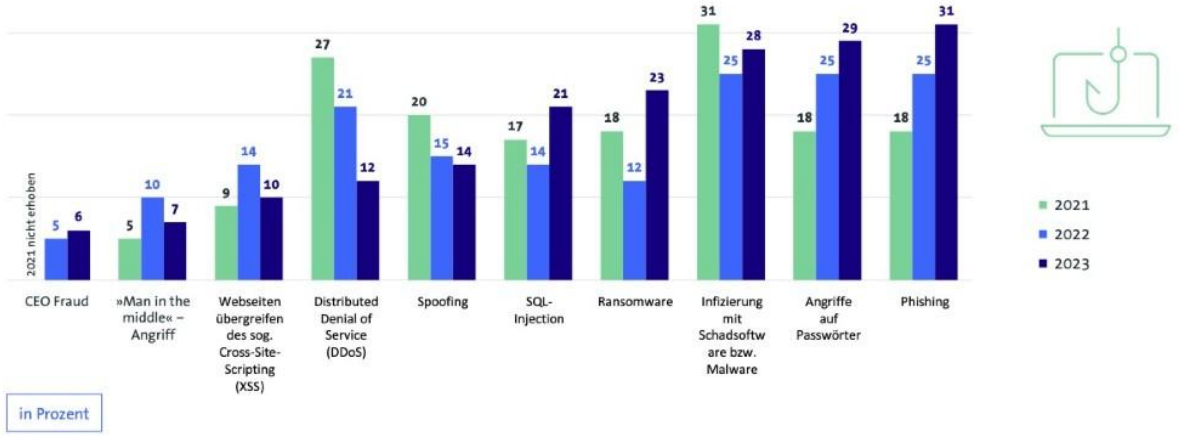
Welche der folgenden Erfahrungen mit kriminellen Vorfällen haben Sie persönlich in den vergangenen 12 Monaten im Internet gemacht?

Basis: 1.018 Internetnutzerinnen und-nutzer ab 16 Jahren in Deutschland | Mehrfachnennungen möglich | Quelle: Bitkom Research 2024

bitkom

Häufige Schäden durch Phishing, Passwortklau & Malware

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?



Basis: Alle Unternehmen (n=1.002) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2023

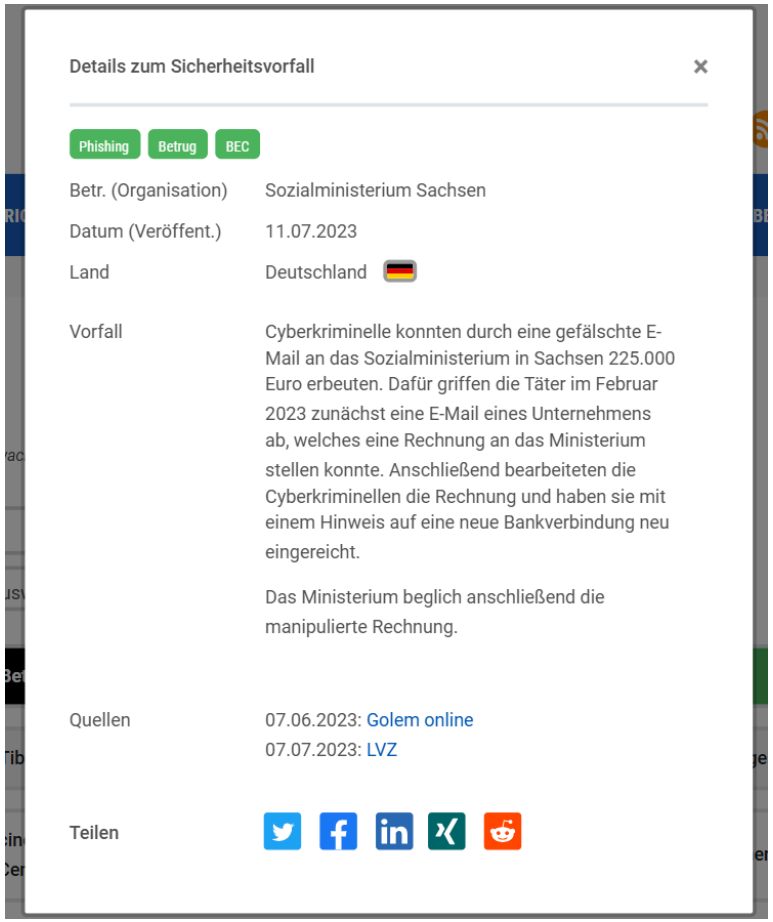
bitkom

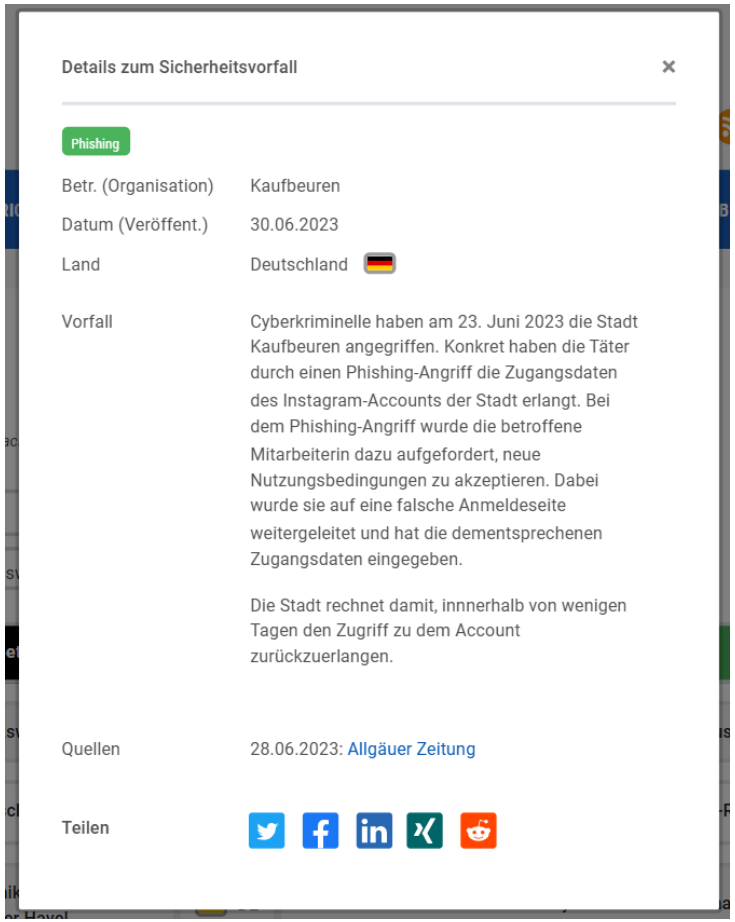
Meldung von Sicherheitsvorfällen

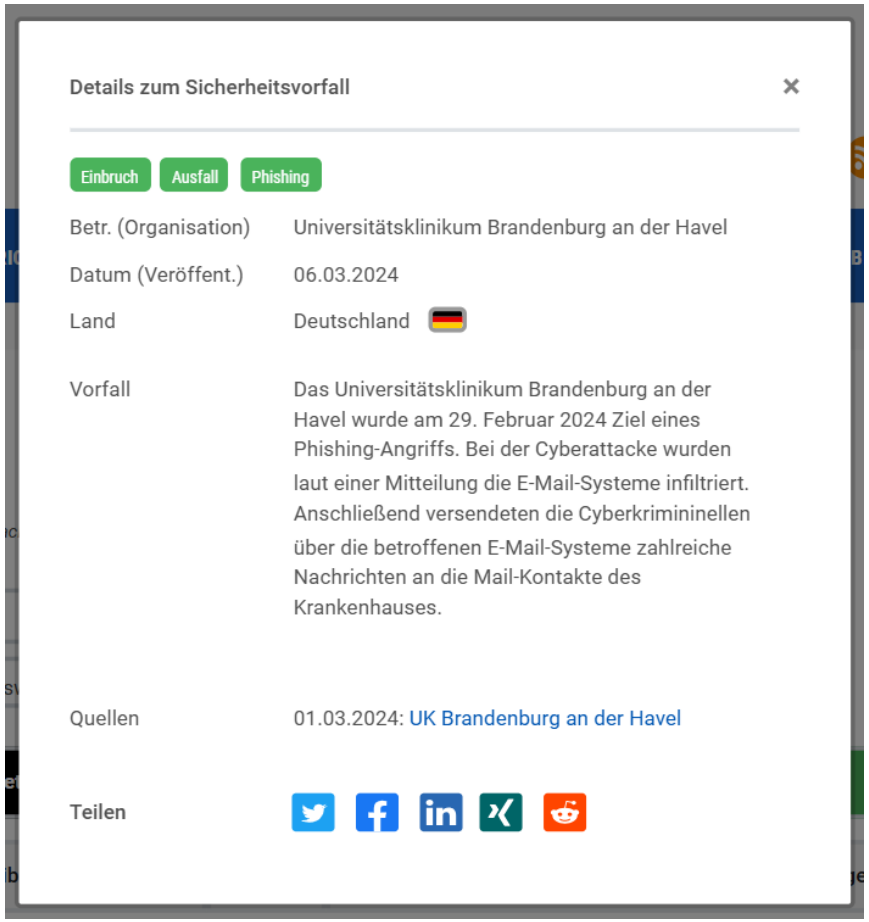
Datum	Betroffene	Land	Sicherheitsvorfall
19.04.2024	Volkswagen	DE	VW jahrelang von chinesischen Staatshackern ausspioniert. » Details
10.04.2024	Mehrere deutsche Unternehmen	DE	KI-gestützte Phishing-Attacke mit infizierten Metro-Rechnungen. » Details
01.03.2024	Universitätsklinikum Brandenburg an der Havel	DE	Hacker infiltrieren IT-System von Krankenhaus. » Details
28.06.2023	Kaufbeuren	DE	Cyberkriminelle erlangen Zugriff zu Instagramkonto von Kleinstadt. » Details
07.06.2023	Sozialministerium Sachsen	DE	Betrüger ergaunern durch manipulierte Rechnung 225.000 Euro. » Details
12.05.2023	Bundesverband der Pharmazeutischen Industrie	DE	E-Mail-Postfächer von Verbandsmitgliedern kompromittiert. » Details
03.04.2023	Üstra	DE	Ransomware-Angriff auf Verkehrsgesellschaft sorgt für Ausfall von Anzeigetafeln und Störungen beim Verkauf des Deutschland-Tickets. » Details
20.02.2023	Landratsamt Böblingen	DE	Cyberkriminelle versenden 200.000 Phishing-Mails über offizielle E-Mail-Adresse. » Details

https://www.dsgvo-portal.de/sicherheitsvorfall-datenbank/
Stand November 2024

Details der drei Beispielvorfälle







Warum ist Phishing so gefährlich?

Das bloße Öffnen einer E-Mail (gemessen am Herunterladen von Bildern) kann dem Angreifer bestätigen, dass diese E-Mail-Adresse tatsächlich bedient wird (aktiv ist), so dass diese für spezifischere Angriffe weiterverwendet werden könnte – auch für Social Engineering.

Durch das Klicken auf den Link in der E-Mail könnte im Hintergrund Schadsoftware von einer Website heruntergeladen werden oder ein Popup geöffnet werden, ohne dass man es merkt. Passen die Rechte des Users, könnte damit ein ganzes Netzwerk beschädigt oder Daten verschlüsselt werden.

Gibt jemand sein Passwort ein, könnte man auf eine grundsätzliche Passwort-Struktur schließen und auch andere Passworte erraten bzw. dieses Passwort auch in anderen Anwendungen nutzen, sollte es gleich sein.

Eingegebene Daten und E-Mail-Adressen könnten im Darknet veröffentlicht oder sogar verkauft werden – Datenschutz- und Sicherheitsproblem gerade im Falle von Bankdaten.

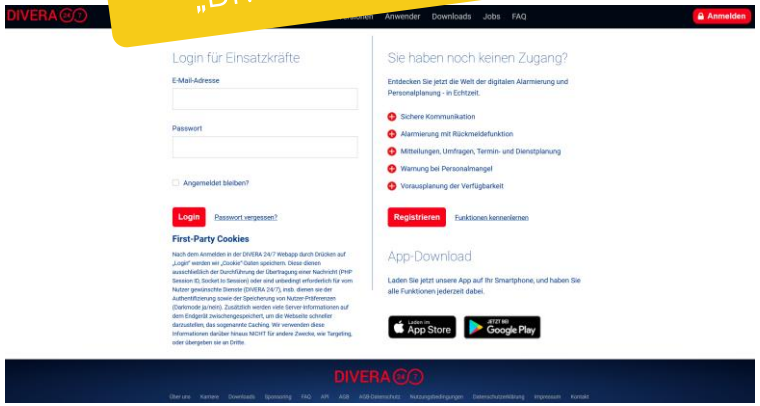
Phishing-Kampagne bei DLRG LV Württemberg

In KW 20 und 21 wurden drei E-Mails an die Empfänger versandt, die jeweils zu diesen drei Landing-Pages gehören, welche dazu verleiten sollen, Daten einzugeben – ganz so, wie es auch bei tatsächlichen Phishing-Angriffen passieren kann.

„Gewinnspiel“

„Paritätischer Wohlfahrtsverband- – Nextcloud“

„Divera 24/7“



E-Mail 1:
12-14. Mai 2025

E-Mail 2:
20. Mai 2025

E-Mail 3:
22. Mai 2025

Öffnungs- Klick- und Eingaberaten

Viele Personen haben die Mails bzw. die Domain der Landings-Pages „geflaggt“ und als Phishing deklariert. Das ist sehr lobenswert.

Außerdem wurde die Kampagne in den internen Messenger-Gruppen des Landesverbands diskutiert und man warnte sich gegenseitig. Auch das ist sehr positiv zu erwähnen!

Template	E-Mails sent	E-Mails opened	Clicked links	Submitted data
Gewinnspiel	3.816	1.914	679	298
Paritätischer Wohlfahrtsverband (NextCloud)	1.916	856	35	10
Divera 24/7	920	173	36	10

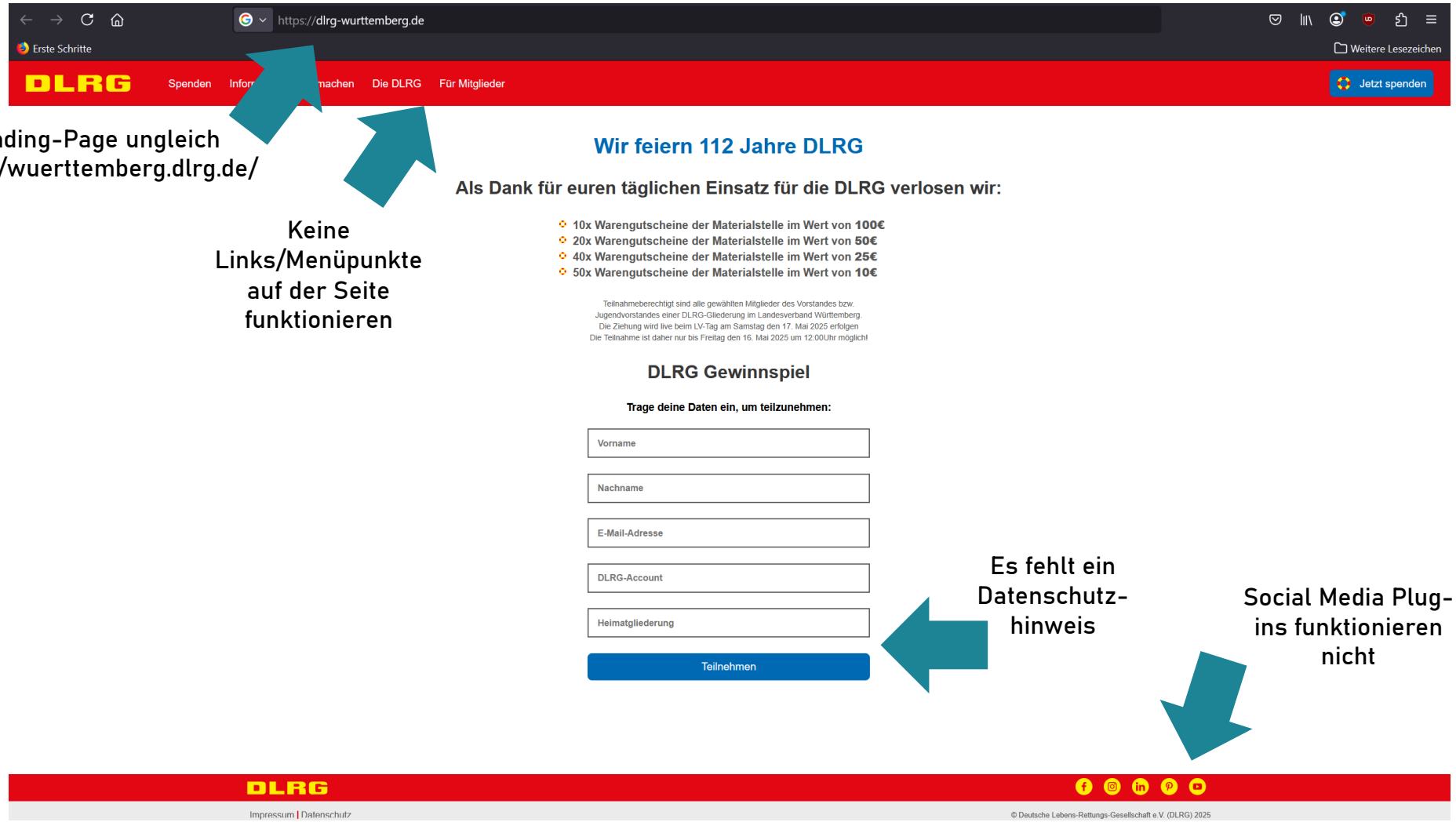
Die Psychologie hinter Phishing

Als Form des Social Engineering wird beim Phishing versucht, psychologische Trigger beim Opfer zu nutzen:

- Druck
- Angst
- Neugier
- Gier
- Vorteile
- Autorität

So kann man Phishing-Mails erkennen…

So kann man Fake-Pages erkennen…



5 typische Merkmale einer Phishing-Mail

sicher3

1. Unpersönliche Anrede & Druckaufbau

- Oft fehlt eine persönliche Ansprache (z. B. „Sehr geehrter Kunde“ statt Name).
- Die Mail erzeugt Stress („Ihr Konto wird gesperrt!“) oder fordert schnelles Handeln („Bestätigen Sie Ihre Daten innerhalb von 24 Stunden“).

2. Verdächtige Absenderadresse

- Die Absenderadresse weicht leicht von der echten Domain ab (z. B. „service@paypa1.com“ statt „service@paypal.com“).
- Manchmal sind ungewöhnliche oder generische Absendernamen zu sehen.

3. Rechtschreib- und Grammatikfehler (passiert immer seltener)

- Manche Phishing-Mails enthalten Tippfehler, falsche Zeichensetzung oder schlechte Grammatik.
- Seriöse Unternehmen, die Mails versenden, prüfen ihre Mails sorgfältig.

4. Auffällige Links & Anhänge

- Links leiten oft auf gefälschte Webseiten um (Tipp: Mit der Maus über den Link fahren, ohne zu klicken – die echte URL wird dann angezeigt).
- Unbekannte oder unerwartete Anhänge (z. B. ZIP-Dateien oder Office-Dokumente mit Makros) sind oft gefährlich.

5. Ungewöhnliche Aufforderungen

- Die Mail verlangt sensible Daten wie Passwörter, Bankdaten oder PINs.
- Banken und seriöse Unternehmen fordern solche Daten nie per E-Mail an.

👉 **Tipp:** Wenn eine Mail verdächtig wirkt, niemals auf Links klicken oder Anhänge öffnen! Stattdessen direkt beim angeblichen Absender nachfragen oder die offizielle Webseite aufrufen. 🚨

Phishing geht auch postalisch!

AOK Baden-Württemberg
Die Gesundheitskasse.

Krankenkasse und Pflegekasse

Versicherung & Beiträge Firmenkunden
Friedrich-Ebert-Straße 30 · 76437 Rastatt

Wir sind immer für Sie da!
Einen Überblick über Kontaktmöglichkeiten, **Terminvereinbarung und unsere Öffnungszeiten** finden Sie unter: www.bw-aok.de/kontakt

Herr David Gallus
Telefon: 0711 6552-14730

13.07.2024

AOK · 76097 Karlsruhe

[redacted]
Personalabteilung
Industriestr. 12
77815 Bühl

Optimierung unserer Dienstleistungen – Ihre Mithilfe ist gefragt!

Sehr geehrte Damen und Herren,

die Zufriedenheit und Gesundheit Ihrer Mitarbeitenden, die bei uns versichert sind, liegt uns sehr am Herzen. Um unsere Dienstleistungen kontinuierlich zu verbessern und bestmöglich auf die Bedürfnisse Ihrer Mitarbeitenden abzustimmen, bitten wir Sie um Ihre Unterstützung.

Wir haben einen kurzen Fragebogen erstellt, der etwa 5 Minuten Ihrer Zeit in Anspruch nimmt. Die gesammelten Informationen werden uns helfen, unsere Leistungen weiter zu optimieren und so noch besser auf die Anforderungen und Wünsche Ihrer Mitarbeitenden einzugehen.

Bitte füllen Sie den Fragebogen unter folgendem Link aus:

https://www.bw-aok.de/optimierung

Ihre Antworten sind uns sehr wichtig und werden selbstverständlich vertraulich behandelt. Durch Ihre Teilnahme tragen Sie wesentlich dazu bei, die Gesundheitsversorgung und den Service für Ihre Mitarbeitenden zu verbessern.

Wir danken Ihnen herzlich für Ihre Unterstützung und Ihr Engagement.

Mit freundlichen Grüßen

David Gallus

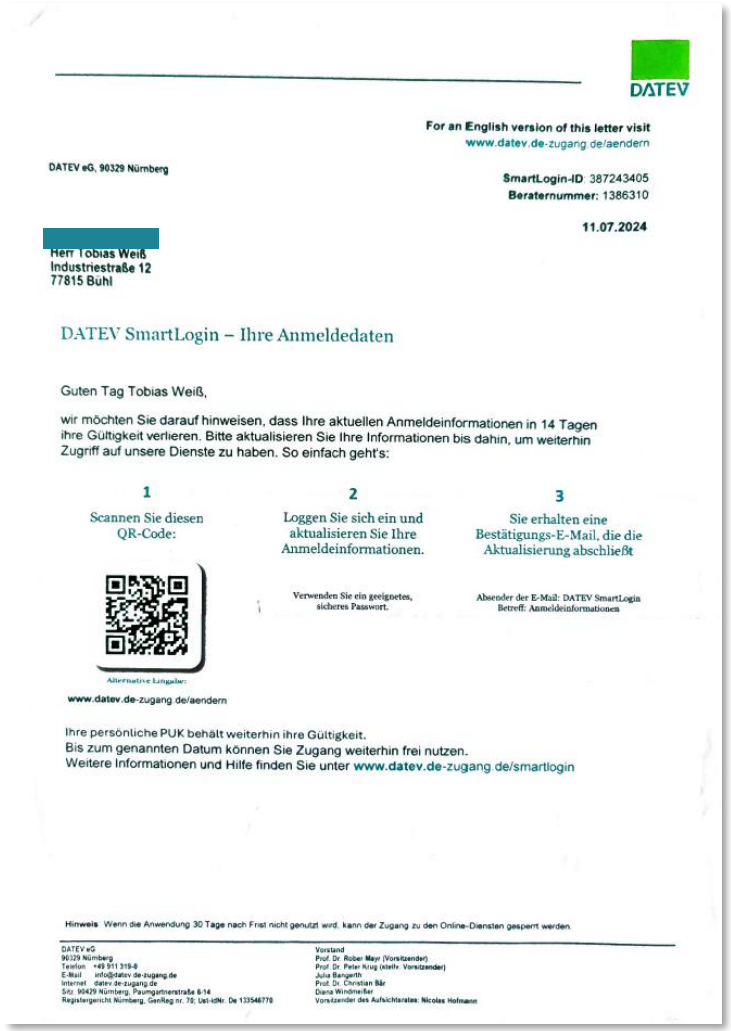
BPMANIFK 75303625

Landesbank Baden-Württemberg
IBAN DE57 6005 0101 0004 0256 00
BIC SOLADEST600

Sparkasse Rastatt
IBAN DE67 6655 0070 0000 0002 57
BIC SOLADES1RAS

Volksbank Karlsruhe
IBAN DE20 6619 0000 0010 0010 30
BIC GENODE61KA1

IK 108918251



DATEV

For an English version of this letter visit
www.datev.de-zugang.de/aendern

DATEV eG, 90329 Nürnberg

SmartLogin-ID: 387243405
Beraternummer: 1386310

11.07.2024

[redacted]
Herr Tobias Weiß
Industriestraße 12
77815 Bühl

DATEV SmartLogin – Ihre Anmeldedaten

Guten Tag Tobias Weiß,

wir möchten Sie darauf hinweisen, dass Ihre aktuellen Anmeldeinformationen in 14 Tagen ihre Gültigkeit verlieren. Bitte aktualisieren Sie Ihre Informationen bis dahin, um weiterhin Zugriff auf unsere Dienste zu haben. So einfach geht's:

1	2	3
Scannen Sie diesen QR-Code:	Loggen Sie sich ein und aktualisieren Sie Ihre Anmeldeinformationen.	Sie erhalten eine Bestätigungs-E-Mail, die die Aktualisierung abschließt
Alternative Eingabe: www.datev.de-zugang.de/aendern	Verwenden Sie ein geeignetes, sicheres Passwort.	Absender der E-Mail: DATEV SmartLogin Betreff: Anmeldeinformationen

Ihre persönliche PUK behält weiterhin ihre Gültigkeit.
Bis zum genannten Datum können Sie Zugang weiterhin frei nutzen.
Weitere Informationen und Hilfe finden Sie unter www.datev.de-zugang.de/smartlogin

Hinweis: Wenn die Anwendung 30 Tage nach Frist nicht genutzt wird, kann der Zugang zu den Online-Diensten gesperrt werden.

DATEV eG
90329 Nürnberg
Telefon +49 911 319-0
E-Mail info@datev.de-zugang.de
Internet datev.de-zugang.de
Sitz: 90429 Nürnberg, Paumgartnerstraße 6-14
Registergericht Nürnberg, GenReg nr. 70; Ust-IdNr. De 13546770

Vorstand
Prof. Dr. Robert Mayr (Vorsitzender)
Prof. Dr. Peter Knog (stellv. Vorsitzender)
Julia Bangerth
Prof. Dr. Christian Bär
Diana Windmeißer
Vorsitzender des Aufsichtsrates: Nicolas Hofmann

Volksbank Bühl

Volksbank Bühl, Friedrichstr. 4, 77815 Bühl

[redacted]
Firma
Industriestr. 12
77815 Bühl

Volksbank Bühl eG
Friedrichstr. 4
77815 Bühl

Telefon 07223 985-0
info@volksbank-buehl.de
www.volksbank-buehl.de

Ansprechpartner:
Team eBanking
Telefon: 07223 985-0
ebanking@volksbank-buehl.de

Datum:
28.11.2023

Aufsichtsratsvorsitzender:
Claus Eckerle

Vorstand:
Marco Feil
Hans-Jörg Meier

Registergericht:
Amtsgericht Mannheim
Genossenschaftsregister Nr. 210014
USt.-IdNr. DE 143752774

Wichtige Mitteilung zur Erhöhung der Online-Banking-Sicherheit

Sehr geehrte Damen und Herren,

in letzter Zeit ist es vermehrt zu Cyberangriffen auf Online-Banking-Accounts gekommen. Die Sicherheit Ihrer Finanzdaten hat für uns höchste Priorität. Daher möchten wir Sie darüber informieren, dass wir zusätzliche Sicherheitsmaßnahmen implementieren, um Ihre Konten bestmöglich zu schützen.

Als Teil dieser Maßnahmen bitten wir Sie, unter dem folgenden Link Sicherheitsfragen zu beantworten:

https://volksbank-buehl.de-zugang.de/sicherheitsfragen

Durch das Beantworten dieser Fragen tragen Sie wesentlich dazu bei, Ihr Online-Banking-Konto vor unbefugtem Zugriff zu schützen. Bitte nehmen Sie sich einen Moment Zeit, um diese wichtigen Sicherheitsfragen zu beantworten.

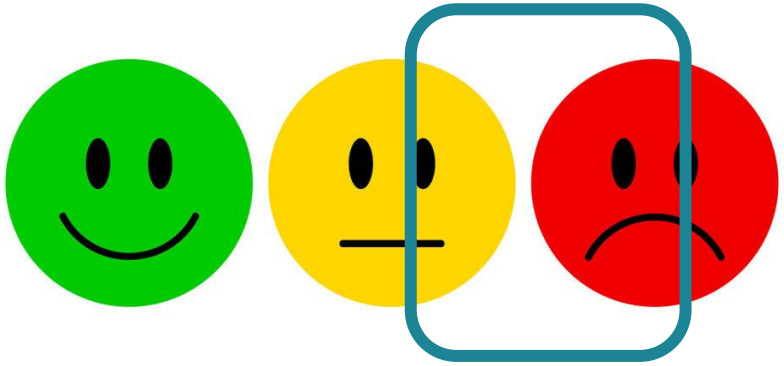
Wir danken Ihnen für Ihre Mithilfe und Ihr Verständnis.

Mit freundlichen Grüßen,

Ihr Team eBanking
Volksbank Bühl eG

Wir machen den Weg frei. Gemeinsam mit den Spezialisten der Genossenschaftlichen FinanzGruppe Volksbanken Raiffeisenbanken.

Dies ist unser Fazit



Die durchgeführte Phishing-Simulation hat gezeigt, dass ein Großteil der angeschriebenen ehrenamtlichen Funktionsträger **zunächst nur unzureichend auf Phishing-Risiken vorbereitet war**. Die hohe Klick- und Eingaberate in der ersten Phase der Kampagne macht deutlich, wie leicht vertraut wirkende E-Mails zu unbedachten Handlungen führen können – insbesondere wenn sie vermeintlich aus dem eigenen Verein stammen.

Nach einem gezielten Hinweis auf die Kampagne zeigte sich ein **klarer Lerneffekt**: Sowohl die Anzahl der Klicks als auch die Eingaben sensibler Daten gingen deutlich zurück. Zwar wurde die zweite Welle an eine kleinere Empfängergruppe versendet, dennoch ist die beobachtete Verhaltensänderung als positiver Entwicklungsschritt zu werten.

Für die Zukunft ist es entscheidend, dass alle Mitglieder – auch und gerade in ehrenamtlichen Funktionen – für den Umgang mit digitalen Nachrichten sensibilisiert bleiben. E-Mails mit vereinsinternem Anschein sollten **stets kritisch geprüft werden**. Die Ergebnisse der Kampagne unterstreichen, wie wichtig regelmäßige Schulungen und wiederkehrende Tests sind, um ein dauerhaft sicheres Verhalten im digitalen Alltag zu fördern.

Besten Dank und bis bald…

sicher 3

jannis.fellinghauer@sicher-hoch-drei.com
julia.dubowy@sicher-hoch-drei.com

www.sicher-hoch-drei.com