

Cybersécherheet doheem

Äre Pocket-Guide géint Phishing, KI-Bedrug a Stëmm-Klon — an
einfache Reflexer fir all Dag.

WAT DRASTEET

1 Phishing & KI

2 Stëmm-Klon & Deepfakes

3 Passwierder & 2FA

4 Är Donnéeën online

5 Schutz-Reflexer

6 Wann eppes geschitt

Erkennt d'Falle — och bei perfekter Sprooch

KI schreift haut feelerfräi — Schreiffeeler erkennen duer net méi. Phishing bleift awer phishing: dës 5 Signaler verrodnen et ëmmer.

5 SIGNALER — OCH BEI KI NACH GËLTEG

1

DROCK & EIL

"Just elo!", "Soss verléiert Dir alles..." — Eil ass eng Waff.

2

ONGEWÉINLECHE KANAL

Är Bank schreift lech net iwwer WhatsApp oder SMS.

3

LINK PRÉIFEN

Maus drop ouni ze klicken — kuckt op den Domain.

4

DIREKT UFRO

Passwuert, Code oder Suen iwwer Mail/SMS — ni.

5

GUTT GEFILL

Wann eppes komescht richt, ass et meeschtens komescht.

AM ZWEIFEL

Klickt op näischt. Maacht d'Säit selwer op (tippt d'Adress) oder rufft op der gewinnter Nummer un. Eng richtig Bank/Administratioun setzt lech ni esou ënner Drock.

Wann d'Aen an d'Oueren lech täuschen

3 Sek

Audio-Material — méi brauch eng KI net fir Är Stëmm ze klonen. Quellen: Voicemail, Telefonsuruff, YouTube, TikTok, WhatsApp-Sproochnoricht.

ÄR HALLEFRÄISCH-LÉISUNG

E Familljen-Codewuert

Setzt mat Äre Kanner an Eltere e Wuert fest, dat nëmme bei lech bekannt ass. Bei all dréngender Geldufro um Telefon: frot no dem Codewuert.

MÉI REFLEXER GÉINT STÄMM-KLON

1

RIFFT ZRÉCK

Op déi gewinnt Nummer — NET op déi vum Uruff.

2

STELLT ENG FRO

Eng Detail déi nëmmen déi richtig Persoun weess.

3

MËSSTRAUT DER EIL

Krimineller setze bewusst Drock op — atmen, nodenken.

4

QUELL PRÉIFEN

Bei Politiker oder Promi: kuckt op déi offiziell Säit.

Är zwou wichtegst Schlässer

80 % vun den Hacker-Attacke kommen vun engem schwaachen oder geklauten Passwuert.

X SCHWAACH

123456 • Marc1980

Crackt a Sekonnen. Datselwecht Passwuert
iwwerall = 1 Lëck a all Är Konten sinn op.

✓ STAARK

Kaffi-Schmaacht-Gutt-2026!

Crackt an iwwer 200 Joer. Mindestens 12
Zeechen, léiwer 16+, eenzegaarteg pro Konto.

DE PASSWUERT-MANAGER — ÄR SCHLËSSELBOND

Ee staarkt Master-Passwuert ze behalen — den Tool mécht de Rescht: späichert all Passwierder verschlüsselt, generéiert komplex Passwierder, fëllt automatesch aus a warnt lech wann e Passwuert geleakt gouf.

2FA — ÄR ZWEET SCHICHT (99,9 % VUN ATTACKE BLOCKÉIERT)

BESCHT

Hardware-Schlëssel (YubiKey) — net duerch Phishing ze ëmgoen.

GUTT

Authenticator-App (Aegis, Authy) — gratis a sécher, empfollen.

OK

Push-Notifikatioun (Microsoft, Google) — bequem, zimlech sécher.

MANNER

SMS-Code — funktionéiert, awer ka geklaut ginn.

Manner online — manner Risiko

WAT BESSER NET ËFFENTLECH DEELEN

- Är voll Adress, Telefonsnummer oder IBAN
- Geburtsdatum — Är an dee vun Äre Kanner
- Vakanz LIVE — éischer no der Heemkonft posten
- Fotoe vu Päss, Karten oder Identitéitspabeier
- Deeglech Routinen ("All Méindes joggen ech...")
- Selfie mat sichtbarer Aarbechtsplaz oder Schoul

D'GOLDREEGEL

"Wier ech bereet, dat hei engem Friemen op der Strooss ze soen?" Wann d'Äntwert NEE ass — dann och net online.

ÄR PRIVATSPHÄR-ASTELLUNGEN — 5 MINUTTEN GUTT INVESTÉIERT

1 PROFIL OP PRIVAT

Nëmme Frënn gesinn Är Posts a Fotoen.

2 FRËNN-LËSCHT CHECKEN

All Joer kuckt no, wien eng Verbindung huet.

3 APP-PERMISSIONEN

Brauch eng Taschelampen-App wierklech Är Kamera?

4 STANDUERT OF

Schalt d'GPS-Markéierung bei Fotoen of.

5 UFROEN MËSSTRAUEN

Onbekannte "Frënn" refuséieren ass keng Onhéiflechkeet.

Gewunnechten déi Iech all Dag schützen

STOP · DENKEN · VERIFIZÉIEREN · HANDELEN

1

STOP

Otemt déif. Klickt op näischt. Äntwert net direkt.

2

DENKT

Wier dat normal? Géif déi Persoun mech sou kontaktéieren?

3

VERIFIZÉIERT

Rufft op déi gewinnt Nummer un — oder frot direkt no.

4

HANDELT

Eréischt wann Dir 100 % sécher sidd.

D'3-2-1 BACKUP-REEGEL — GÉINT RANSOMWARE & VERLUST

3

Kopien

vun Äre wichtege Donnéeën

2

Medien

z.B. extern Festplack + Cloud

1

Aner Plaz

ausserhalb vun doheem

ÄR DIGITAL HYGIÈNE

UPDATE

Software regelméisseg aktualiséieren — Updates fixéieren Sécherheets-Lächer.

ANTIVIRUS

Schutz aschalten — Windows Defender geet duer fir d'meescht Privatleit.

WIFI

Ëffentlech Netzwierker mat Virsicht — sensibel Saachen iwwer Mobile-Data/VPN.

AL APPARATER

Ofschalten wat keng Updates méi kritt — en aalen Apparat ass eng oppen Dier.

Roueg bleiwen, séier handelen

ÄR 5-SCHRÉTT-REAKTIOUN

1

BLEIFT ROUEG

Panik mécht alles méi schlëmm. Otemt — denkt.

2

TRENT D'VERBINDUNG

Internet aus, Apparat ofschalten wann néideg.

3

ÄNNERT PASSWIERDER

Vun engem aneren, sécheren Apparat.

4

KONTAKTÉIERT D'BANK

Wann Geld am Spill ass — direkt!

5

MELLT ET

BEE SECURE · Police 113 · CIRCL · NC3.

WOU KRITT DIR HËLLEF ZU LËTZEBUERG?

BEE SECURE**8002-1234**

Anonym a gratis. Phishing, Mobbing, Hack.

bee-secure.lu**CIRCL.lu****247-88444**

Incident Response — séier Hëllef bei Attacken.

circl.lu**POLICE****113**Dréngend Fäll. Plainte op police.lu.police.lu**NC3****274 00 98 601**

Trainings, Guiden & Ressourcen.

nc3.lu

7 Reflexer fir Är Cyber-Hygiène

1	KI mécht d'Attacken realistesch	Net méi un Schreiffeeler z'erkennen
2	Setzt e Familljen-Codewuert	Schützt géint Stëmm-Klon-Bedrug
3	Manner online = manner Risiko	Spuert mat ëffentlechen Donnéeën
4	Ee Passwuert pro Site + Manager	Ni datselwecht iwwerall
5	2FA op all wichtige Kont	Bank, Mail, sozial Medien
6	Stop · Denken · Verifizéieren · Handelen	Bei all dréngender Ufro
7	Backups + Updates regelméisseg	Är Versécherung géint d'Schlëmmst

RESSOURCEN

● nc3.lu

National Cybersecurity Competence Center

● circl.lu

Incident Response — bei Hack: rufft un!

● cnpd.lu

Datenschutzkommissioun — Är RGPD-Rechter

● bee-secure.lu

Sensibiliséierung — Helpline 8002-1234

● govcert.lu

Cyber-Sécherheet vum Lëtzebuurger Staat

● police.lu

Plainte deposéieren — Bedrug & Erpressung