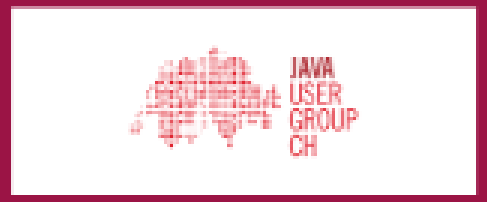

helvetia

KARAKUN

Kanton Basel-Stadt

ERNI

INNOFUSE


Basel
basel.ch

JAVA
USER
GROUP
CH

BLKB

optravis
company of msg

cyon

CS2

CSS

IRIX

swiss made
software

ICT
Scouts
Wir fördern Zukunft

SD



HELP, I SPAMMED!
EMAIL SECURITY FOR SMES

Why trust is vulnerable – and how we protect it!

Adrian Etter – CTO
Kevin Illi – Cyber Security Specialist

Silenccio AG

Agenda

- Situation – Why are we here?
- Problem #1 – Your reputation is on fire!
- Problem #2 – Your password!
- Problem #3 – No plan is no plan!
- Problem #4 - Trust needs control
- Q&A – Your questions

SPAM

~~NOT TODAY~~



STATE OF SCAMS - USA



22 %



$64.8B



$1'086

Source: GASA Global Anti-Scam Alliance, US Report

„I CAN ALWAYS RECOGNISE A SCAM!“

$1’406 lost



Source: GASA Global Anti-Scam Alliance, Switzerland Report

„I RECOGNISE EVERY SCAM!“

CHF 713 lost

58%

of scams by email

Source: GASA Global Anti-Scam Alliance, Switzerland Report

PROBLEM #1

Your reputation is on fire!

TRUST

Brand • Name • Reputation

From: CSS g@[redacted]er.ch
Subject: Prämienabrechnung in myCSS
Date: 3 September 2025 at 15:38
To: adrian.etter@digitalimpact.ch

CSS

Prämienabrechnung in myCSS

Nach den aktuellen Berechnungen Ihrer Krankenkasse freuen

0h – normal

24h – Chaos

48h – Reputational damage

COULD THIS HAPPEN TO ME?

NO SECURITY VULNERABILITY – JUST OPEN

SPF DKIM
DMARC

SPF

WHO MAY SEND?

DKIM

IS THE MAIL GENUINE?

DMARC

WHAT TO DO ON FAILURE?

WHO – GENUINE – WHAT TO DO

THIS IS NOT A HACK.

Unless it’s in your Sent folder

PROBLEM #2

Your password!

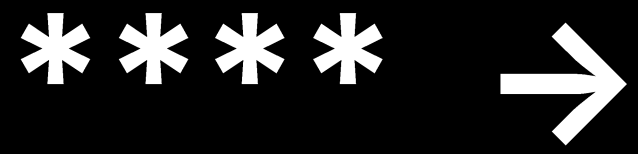




VOUCHER / GIFT CARD



FAMILIAR-LOOKING SENDER



PASSWORD MANAGER

Password manager

Unique

2FA

PROBLEM #3

No plan is no plan!

NOW PREPARATION COUNTS

NO GLYPH EMERGENCY CONTACT KNOWN
NO GLYPH FIRST STEPS DEFINED
NO GLYPH PRACTISED – NOT JUST KNOWN

Learning is applied action.

ACTION = SECURITY



PROBLEM #4

Trust needs control

AUTOMATED.
EVERYTHING.

AUTOMATION WITHOUT MONITORING IS AN OPEN GATE.

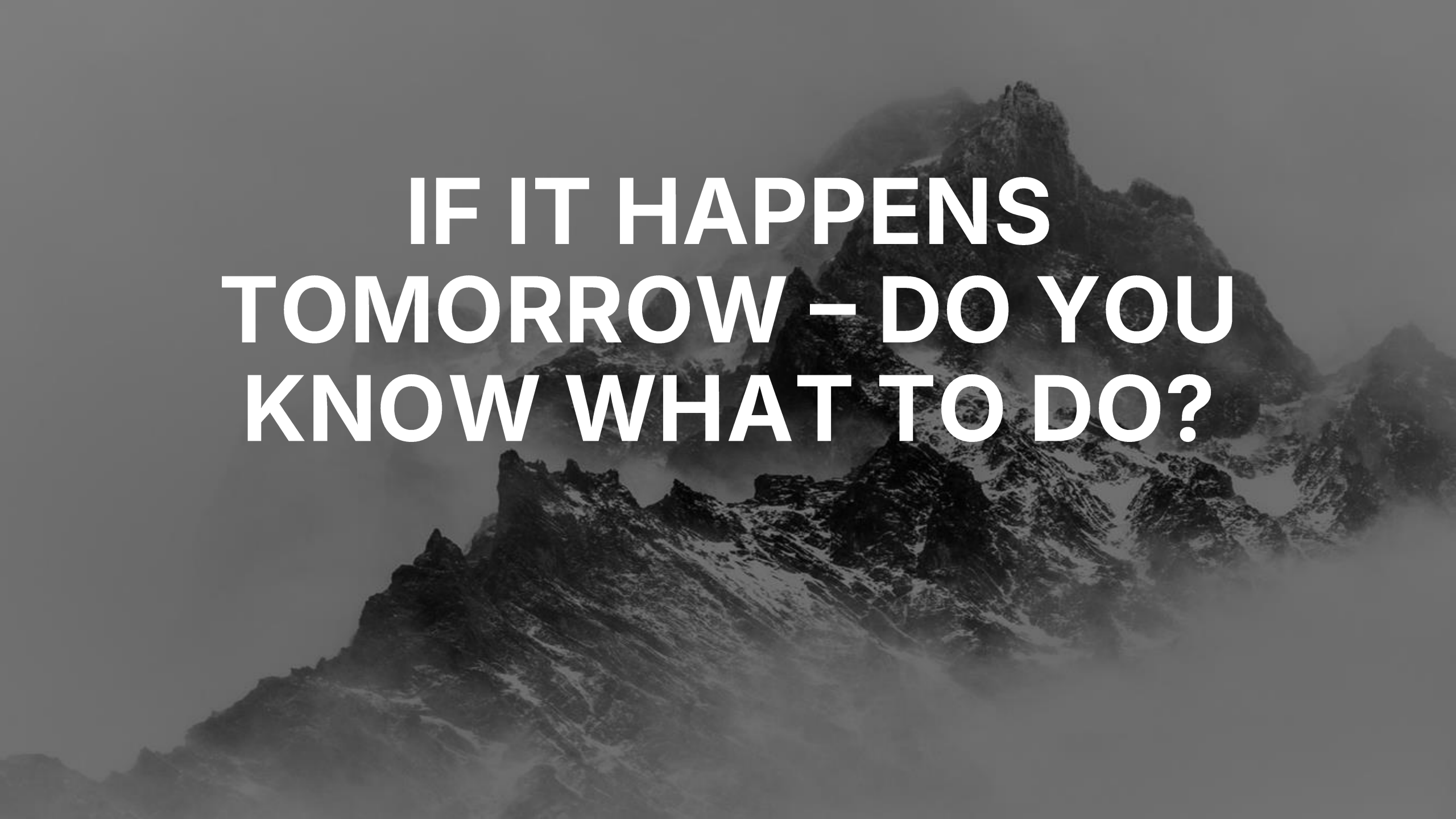
… AND MAYBE CYBER INSURANCE …

TAKE AWAYS

Trust

Email Hardening

Preparation


IF IT HAPPENS
TOMORROW – DO YOU
KNOW WHAT TO DO?

To Do’s

#1 YOUR REPUTATION IS YOUR DOMAIN, SPF · DKIM · DMARC – SET IT UP TOMORROW, NOT SOMEDAY!

#2 ONE PASSWORD IS NO PASSWORD – PASSWORD MANAGER. UNIQUE. 2FA ON.

#3 PREPARATION BEATS PANIC – KNOW AN EMERGENCY CONTACT. HAVE A PLAN.

#4 TRUST NEEDS VERIFICATION – AUTOMATION WITHOUT MONITORING IS AN OPEN GATE.


IF IT HAPPENS
TOMORROW – YOU
KNOW WHAT TO DO!

THANK YOU VERY MUCH

Questions? Now. At the apéro. Or later

Axa Cyberalarm Schweiz

Feedback

Help, I've Been Spamming!



Adrian Etter

CTO | Cyber Security & AI Risk | Cyber Defence, Resilience & Secure Architecture | S...



Kevin Illi

Cyber Security Specialist @ Silenccio | OSCP | OSEP | CISSP

APPENDIX

SPF: include & redirect

How mechanisms combine – and where it goes wrong

include:

Borrows another domain's SPF policy and folds the result into your own evaluation.

Sub-result	Effect on parent
pass	include matches → continue
fail / softfail	include doesn't match → next
neutral (?all)	include doesn't match → next
permerror / none	parent returns permerror

✓ **A -all always has the final word**

⚡ Each include counts as 1+ DNS lookup (recursive!)

redirect=

Replaces your entire SPF record with another domain's policy.

✓ Works only if no -all / ~all / ?all / +all present

✓ Entire target record is used as-is – their all is final

✗ If all exists in your record, redirect is silently ignored

✗ No fallback – if target domain has no SPF, permerror

⚡ Counts as 1 DNS lookup; target record may add more

⚠ Common Problems

10-lookup limit
ip4/ip6 are free. Everything else counts: include, a, mx, ptr, exists. Recursive includes multiply fast. Exceeding = permerror = fail.

?all in an include
A 3rd party using ?all means unlisted IPs return neutral. A -all catches it, but the include provides zero protection on its own.

redirect + -all = dead redirect
If you write both redirect= and -all in the same record, redirect is completely ignored. Silent no-op.

include chain break
If any domain in your include chain has no SPF record, evaluation returns permerror – not fail. Your emails may be rejected.

Email Auth Cheat Sheet

dig commands · online tools · what to look for

SPF

Sender Policy Framework – who may send for your domain

```
dig +short TXT example.com                → look for v=spf1 ...
dig +short TXT _spf.example.com           → some providers use subdomains
```

✓ Expect: v=spf1 ... -all ⚠ Watch for: ?all / ~all / >10 DNS lookups

DKIM

DomainKeys Identified Mail – cryptographic signature per message

```
dig +short TXT selector._domainkey.example.com   → need selector first
```

Try: `google` `mail` `smtp` `k1` `s1` `s2` `mailjet` `sendgrid` `amazonses` `protonmail`

✓ Expect: v=DKIM1; k=rsa; p=<long key> ⚠ Empty p= means key is revoked

DMARC

Domain-based Message Authentication – policy + reporting

```
dig +short TXT _dmarc.example.com         → always _dmarc prefix
```

p=none	p=quarantine	p=reject
monitor only	→ spam folder	block – goal state

✓ Also verify: rua= (aggregate reports) and ruf= (forensic reports) are set

Online Tools

MXToolbox — mxtoolbox.com
- · SPF / DKIM / DMARC lookup
- · Blacklist check (200+ lists)
- · Email header analyzer
- · DNS health report

Best all-round starting point

mail-tester.com — mail-tester.com
- · Send real email → get score /10
- · Checks SPF + DKIM + DMARC
- · Content + spam filter check

Gold standard for deliverability

dmarcian — dmarcian.com
- · DMARC record inspector
- · Visualize rua report data
- · Policy rollout guidance

Best for DMARC deep dives

learndmarc.com — learndmarc.com
- · Interactive auth simulator
- · Great for explaining to clients

Perfect for live demos

Replace example.com with your domain · DKIM selector: check mail provider settings or look for DKIM-Signature: s=... in raw email headers

Spoofing Test with swaks

Can your domain be spoofed right now? Test it yourself – ethically, on your own domain.

⚠ **Only test domains you own or have explicit permission to test. swaks sends real SMTP traffic.**

Step 1 — Set your variables

```
export MX_SERVER=yourdomain.com          → domain to impersonate
export MAIL_TO=you@yourpersonal.com      → where you want to receive the test
```

Step 2 — Send the spoofed test mail

```
swaks \
  --to ${MAIL_TO} \                                  envelope recipient
  --from test@${MX_SERVER} \                         envelope sender – spoofed
  --server $(dig MX ${MX_SERVER} +short \            resolves target MX
    | head -1 | awk '{print $2}') \
  --header "From: Test <something@${MX_SERVER}>" \   visible From: header
  --header "Subject: Test Mail" \
  --header "MIME-Version: 1.0" \
  --header "Content-Type: text/html; charset=UTF-8" \
  --body @mail.html                                  any HTML file works
```

Step 3 — Check your inbox – what happened?

✓ Lands in inbox
Vulnerable – SPF too permissive or DMARC not enforced

~ Goes to spam
Partial – ~all SPF or DMARC quarantine active

✗ Rejected
Protected – DMARC p=reject or -all enforced

What this tests

SPF enforcement
Does the receiver verify the envelope sender IP against your SPF record?

DMARC policy
Is p=reject / quarantine enforced, or just p=none (observe only)?

Header From spoofing
Can the visible From: differ from envelope sender and still deliver?

Open relay check
Does the target MX accept mail from arbitrary external senders?

Install swaks

```
brew install swaks
apt install swaks   |   swaks.org
```

swaks = Swiss Army Knife SMTP · Sends real SMTP traffic · Use responsibly on your own infrastructure only

QUESTIONS & ANSWERS

«Our hosting provider set everything up, so we should be safe, right?»

Probably not completely. Hosting providers configure SPF and DKIM for their own infrastructure — that is, for mails that run *through them*. But they don't add DMARC for you, other services that send on your behalf (Mailchimp, Zendesk, Salesforce) are not covered, and they often use `redirect=` — which hands over control of your SPF policy completely. You have to know yourself everything that sends under your domain, and own the policy yourself.

„We have DMARC p=reject, we're protected"

Against unauthenticated spoofing attempts, yes. But p=reject without monitoring (rua=) means you're flying blind — you don't know whether legitimate mails are being rejected. Many companies switch to reject immediately and then wonder why their invoices don't arrive. Correct order: first p=none, collect reports, then quarantine, then reject.

„Isn't SPF enough? Why do we also need DMARC?"

SPF only checks the envelope sender — that is the technical MAIL FROM address in the SMTP dialogue, not the From: line the recipient sees. An attacker can set any envelope and still use a forged visible sender address. DMARC links authentication to the visible From: header and gives you an enforceable policy plus reporting. SPF alone is no spoofing protection for the end user.

„Doesn't a DKIM signature prove that the mail is legitimate?"

DKIM proves that the mail was not tampered with in transit and that the signing key matches the domain record. It does not prove that the sender in the From header is the real one. And if an old selector key is still published in DNS even though it is no longer actively used, it can be abused. Revoke old keys — set p= to empty.

„We're a small company — who would attack us?"

Most attacks are not targeted. Spoofing infrastructure is automated — attackers scan for domains with weak SPF or missing DMARC and send bulk mail from there, because it gets past spam filters. You are not being targeted specifically, you are simply part of the pool. And: supplier fraud increasingly targets SMEs deliberately, precisely because email authentication is weak and internal processes are informal.

„What about subdomains?"

Good question. DMARC has an sp= tag for subdomain policy. Without an explicit value, subdomains inherit the root policy — which sounds good until you realise that mail.einedomain.ch or newsletter.einedomain.ch can still be spoofable if they are not configured correctly. Explicitly set sp=reject.

„Can't we just set everything to reject today?"

Only if you know for certain everything that sends under your domain. Salesforce notifications, ticketing system, newsletter tool, monitoring — anything that is not in the SPF and has no DKIM will immediately start bouncing. The safe way: first p=none with rua=, read the aggregate reports, then step up gradually.

„Which free tool can read DMARC reports?"

The raw reports are XML and not readable by hand. Postmark's DMARC Digests, Dmarcian's Free Tier or Cloudflare's free DMARC management are good entry points for SMEs. The point: rua= is useless if nobody reads the reports.

„Does swaks sound dangerous — should participants really run it?"

It should only be used for domains you are authorised for – and the whole point is: if the configuration is correct, it is supposed to fail. If the mail lands in the inbox, that is the learning moment. The tool itself is decades old and standard in mail server debugging.

„Microsoft 365 / Google Workspace — doesn't that handle everything automatically?"

These platforms configure DKIM and SPF for mails that run through them, yes. But DMARC for your domain is your DNS record — nobody adds that for you. And if you use another service besides M365 that sends under your domain, it must also be in the SPF and have DKIM configured, otherwise DMARC will start rejecting those mails as soon as you step up from p=none.

„What is the one thing I should do this week?"

Add this DNS record:

```
_dmarc.einedomain.ch  TXT  "v=DMARC1;
p=none;
rua=mailto:dmarc@einedomain.ch"
```

Monitoring only, no enforcement, no risk. Then read the first report that arrives. You will probably be surprised by everything that sends under your name.