BRIGHOUSE SECURITY LABS

Creator Security Snapshot Report

Fictional public sample for creators, coaches, educators and online brands

FICTIONAL SAMPLE — NOT A CLIENT ASSESSMENT

All names, accounts, domains, observations and evidence are fabricated. The purpose is to demonstrate BrighouseSec report structure, risk language, prioritisation and practical remediation guidance for creator-led brands.

SAMPLE TARGET	Example Finance Creator — creator.example
DOCUMENT ID	BSL-SAMPLE-CREATOR-002
REPORT TYPE	48-Hour Creator Security Snapshot / Public-Facing Trust Review
PREPARED BY	Brighouse Security Labs / BrighouseSec
CLASSIFICATION	Public sample / fictional / non-confidential
CONTACT	sales@brighousesec.com

No passwords. No login access. No account access. Clear written recommendations.

Important Sample Notice

This document is a fictional public sample. It must not be interpreted as a security assessment of any real creator, business or online brand. The example accounts, domains and observations are placeholders for demonstration only.

A real BrighouseSec Creator Security Snapshot begins only after written scope, target confirmation, authorisation and payment confirmation. BrighouseSec does not request passwords, two-factor authentication codes, inbox access, social media logins or direct account control for this review type.

Executive Summary

This Creator Security Snapshot demonstrates how BrighouseSec would communicate practical, low-touch security observations to a creator-led business. The fictional scenario assumes a finance creator or online educator with a public website, newsletter, social profiles, brand partnership routes and a custom domain used for business enquiries.

The simulated review identified a high creator-security risk posture. The most important themes are account recovery dependency, email/domain trust, impersonation exposure, public contact-route clarity, connected-app review and sponsorship/payment workflow hygiene. These issues are common in fast-growing creator businesses and can normally be improved without technical expertise.

OVERALL SAMPLE RISK	ACTION REQUIRED	TECHNICAL DIFFICULTY
High	**Yes**	**Low**
creator trust exposure	first 24 hours	guided checklist

Creator-Facing Priority Actions

PRIORITY	ACTION	REASON	SUGGESTED OWNER
1	**Secure the account recovery chain**	Reduces takeover risk across YouTube, email, payment and newsletter platforms	Creator / Manager
2	**Confirm SPF, DKIM and DMARC**	Reduces spoofed brand emails and fake sponsorship approaches	Domain / Email owner
3	**Standardise official contact routes**	Makes impersonation and fake outreach easier to spot	Creator / Operations
4	**Review connected apps and delegated access**	Removes old access paths from agencies, editors and third-party tools	Creator / Assistant
5	**Document payment and sponsorship verification rules**	Prevents fake invoices, fake brand deals and audience-facing scams	Creator / Finance

Scope and Limitations

SCOPE-FIRST MODEL	For a real review, BrighouseSec confirms public assets, target accounts, restrictions and delivery expectations in writing before any work begins.
REVIEW STYLE	Low-touch public-facing review. No passwords, no account access, no two-factor codes, no inbox access and no social-media login access.
SAMPLE ASSUMPTION	A creator-led brand requested a lightweight security snapshot before a sponsorship push, product launch, course release or audience growth campaign.

Sample Assets in Scope

ASSET	PURPOSE	REVIEW TYPE
creator.example	**Official creator website and business domain**	Public website and domain trust review
Social profiles	**YouTube, Instagram, TikTok, X and LinkedIn public presence**	Public visibility and impersonation review
Newsletter / link page	**Public subscription and call-to-action routes**	Contact-route clarity review
Business email domain	**SPF, DKIM, DMARC and MX posture**	Passive DNS configuration review
Sponsor/payment workflow	**Publicly stated payment and partnership process**	Process clarity and fraud-resistance review

Out of Scope for This Sample

- No private account access, passwords, authentication credentials or two-factor authentication codes.
- No email inbox access, direct message access, social media logins or creator platform control.
- No phishing, social engineering, password spraying, credential testing or account takeover attempts.
- No intrusive vulnerability scanning, exploitation, destructive testing or attempts to access data.
- No guarantee that all impersonation, brand-abuse or platform risks would be found.

Methodology

PHASE	OBJECTIVE	EXAMPLE ACTIVITIES
1. Scope validation	**Confirm the official brand, accounts and public assets**	Target list, scope statement, authorised public assets, restrictions
2. Public presence review	**Map public trust signals and contact routes**	Website, bios, link pages, newsletters, visible business email routes
3. Domain trust checks	**Review email and DNS trust posture**	SPF, DKIM, DMARC, MX and domain alignment observations
4. Impersonation exposure review	**Identify public signals that make fake accounts easier to run**	Name consistency, account verification signals, fake account warning routes
5. Access hygiene checklist	**Identify account controls that should be verified by the creator**	2FA type, recovery chain, backup codes, old sessions, connected apps
6. Prioritised reporting	**Convert observations into a clear action plan**	Risk rating, business impact, owner, fix guidance and verification steps

Evidence Handling

- Evidence should be sufficient to explain the observation without exposing private account data.
- Public screenshots and command output should be redacted where needed before delivery.
- In this sample, all evidence is fictional and should be treated as formatting demonstration only.

Risk Rating Model

Findings are prioritised using a practical combination of account takeover likelihood, impersonation risk, audience trust impact, public exposure and remediation effort. The priority rating is designed for creator-led businesses that may not have a technical team.

RATING	DEFINITION	TYPICAL RESPONSE EXPECTATION
High	**A weakness that could directly affect account access, revenue, audience trust, sponsor trust or public reputation.**	Address immediately or within 24 hours.
Medium	**A weakness that increases exposure, makes recovery harder or gives impersonators more room to operate.**	Address within 7 days or before the next campaign.
Low	**A hygiene improvement with limited direct impact but useful long-term risk reduction.**	Fix during the next planned account or website review.
Informational	**Useful context or positive observation that does not represent a direct weakness.**	Track as improvement guidance.

Risk Register

ID	FINDING	SEVERITY	AREA	PRIORITY
F-01	**Recovery chain over-dependent on one primary email**	High	Account recovery	Immediate
F-02	**Email/domain trust not enforcing protection**	High	Domain trust	Immediate
F-03	**Impersonation exposure from finance/business content**	High	Brand trust	Ongoing
F-04	**Official contact routes inconsistent across platforms**	Medium	Public contact	7-day fix
F-05	**Connected apps, sessions and delegated access unreviewed**	Medium	Account access	7-day fix
F-06	**Sponsor/payment verification workflow not clearly documented**	Medium	Commercial process	7-day fix

Risk Distribution

HIGH	MEDIUM	LOW
3	**3**	**0**
trust and access issues	process and hygiene	none in sample

F-01 HIGH Recovery chain over-dependent on one primary email

RISK SCORE	AREA	PRIORITY	REVIEW TYPE
High	Account recovery	Immediate	Guided external

OBSERVATION

The sample review assumes one primary email account is used as the login or recovery address for YouTube, Instagram, newsletter, payment tools and brand enquiries.

BUSINESS IMPACT

If this primary mailbox is compromised, an attacker may be able to reset passwords across multiple business-critical services. For a creator-led brand, this can affect channel access, revenue, sponsor communication and audience trust at the same time.

SAMPLE EVIDENCE

```
primary email used for: creator@example.com
linked services: YouTube, newsletter, payment tool, link page, sponsor inbox
recovery method: to be verified by creator during guided checklist
```

RECOMMENDED REMEDIATION

- Review recovery email, phone number and backup methods for the primary mailbox.
- Use app-based 2FA, passkeys or hardware keys rather than SMS where possible.
- Store backup codes offline and separate from the primary email account.

F-02 HIGH Email/domain trust not enforcing protection

RISK SCORE	AREA	PRIORITY	REVIEW TYPE
High	Domain trust	Immediate	Guided external

OBSERVATION

The fictional creator domain does not have a mature SPF, DKIM and DMARC enforcement posture. The sample assumes the domain is used for sponsorships, invoices and business enquiries.

BUSINESS IMPACT

Weak email authentication allows impersonators to send messages that appear to come from the creator brand. This can lead to fake invoices, fake sponsorship requests, phishing messages or audience scams using the creator's credibility.

SAMPLE EVIDENCE

```
dig +short TXT _dmarc.creator.example
"v=DMARC1; p=none"
DKIM alignment: not confirmed in sample
```

RECOMMENDED REMEDIATION

- Confirm all legitimate email senders and enable DKIM signing.
- Move DMARC gradually from p=none to p=quarantine, then p=reject once delivery is stable.
- Use one official domain-based business email for partnerships and public enquiries.

F-03 HIGH Impersonation exposure from finance/business content

RISK SCORE	AREA	PRIORITY	REVIEW TYPE
High	Brand trust	Ongoing	Guided external

OBSERVATION

Finance, business and education creators are high-value impersonation targets because audiences may be more likely to act on investment, money or business-related messages.

BUSINESS IMPACT

A fake account can damage audience trust even if the real creator’s accounts are secure. Scammers may use copied branding, profile images, comments or direct messages to run investment scams, fake giveaways or fake paid communities.

SAMPLE EVIDENCE

```
public niche: finance education
impersonation risk: high audience trust + money-related content
official account list: not clearly centralised in sample
```

RECOMMENDED REMEDIATION

- Publish one official page listing all real accounts and contact routes.
- Add regular public reminders that the creator will not DM investment offers or request money through unofficial channels.
- Save platform impersonation reporting links so incidents can be reported quickly.

F-04 MEDIUM Official contact routes inconsistent across platforms

RISK SCORE	AREA	PRIORITY	REVIEW TYPE
Medium	Public contact	7-day fix	Guided external

OBSERVATION

The sample public presence uses multiple contact routes across the website, social bios, link page and newsletter footer. Not all routes point back to the same official business email.

BUSINESS IMPACT

Inconsistent contact routes create ambiguity. That ambiguity makes fake sponsorship emails, fake collaboration offers and lookalike domains more convincing to brands, viewers and partners.

SAMPLE EVIDENCE

```
website contact: hello@creator.example
Instagram bio: DM for collabs
newsletter footer: partnerships@creator.example
link page: third-party form only
```

RECOMMENDED REMEDIATION

- Choose one official business email and use it everywhere.
- List official contact routes clearly on the website, not only in social bios.
- Remove vague “DM for business” language where sponsorship or payment is involved.

F-05 MEDIUM Connected apps, sessions and delegated access unreviewed

RISK SCORE	AREA	PRIORITY	REVIEW TYPE
Medium	**Account access**	**7-day fix**	**Guided external**

OBSERVATION

Creator businesses often accumulate scheduler tools, analytics platforms, editors, agencies, newsletter integrations and delegated managers over time. The sample assumes these have not been reviewed recently.

BUSINESS IMPACT

Old integrations and delegated users remain active access paths. A compromised third-party tool or forgotten editor account may still be able to modify content, access analytics or act on behalf of the creator.

SAMPLE EVIDENCE

```
connected tools: scheduler, analytics, newsletter, editing workflow
delegated access: agency/editor permissions to be verified
session review: not recently documented in sample
```

RECOMMENDED REMEDIATION

- Review connected apps across YouTube, Meta, TikTok, X, newsletter and payment tools.
- Remove access for old agencies, former editors and unused tools.
- Set a quarterly reminder to review delegated access and active sessions.

F-06 MEDIUM Sponsor/payment verification workflow not clearly documented

RISK SCORE	AREA	PRIORITY	REVIEW TYPE
Medium	**Commercial process**	**7-day fix**	**Guided external**

OBSERVATION

The sample creator brand does not clearly document how sponsors, agencies or audience members can verify payment requests, invoices or official partnership messages.

BUSINESS IMPACT

Without a verification process, scammers can send fake invoices, fake brand-deal requests or fake payment links that appear to involve the creator. This is a commercial trust issue, not just a technical issue.

SAMPLE EVIDENCE

```
official invoice process: not public in sample
payment verification route: not documented
sponsor workflow: multiple contact routes observed
```

RECOMMENDED REMEDIATION

- Document a simple “official payment and sponsorship process” on the website.
- Use domain-based email for invoices and contracts, not personal addresses or DMs.
- Add a rule that payment links and invoice changes are confirmed through the official email channel only.

30-Minute Fix Plan

WHEN	ACTION	OWNER
First 10 minutes	**Review primary email recovery, 2FA method, backup codes and recent login activity.**	Creator
Next 10 minutes	**Review connected apps, active sessions and delegated access across key platforms.**	Creator / Assistant
Final 10 minutes	**Standardise public contact routes and document official sponsorship/payment rules.**	Creator / Operations
Within 7 days	**Improve SPF, DKIM and DMARC with the domain/email provider and centralise official account links.**	Domain / Email owner

What a Client Receives

- A concise PDF report written for creators, managers and non-technical business owners.
- A clear list of public-facing risks that can affect account access, audience trust and sponsor confidence.
- Practical remediation steps that do not require sharing passwords or giving account access.
- A fixed written scope before work begins and no intrusive testing without explicit approval.
- Optional follow-up guidance after fixes or before a major launch, campaign or sponsorship push.

Positioning Note

This sample is designed to show how BrighouseSec communicates creator-security findings without exposing real client data. In a real engagement, target names, screenshots, logs and observations would only be shared with the authorised recipient and would not be published without explicit written permission.

End of Sample Report

Brighouse Security Labs provides low-touch external security snapshots, creator security reviews and written remediation plans for creator-led brands, online educators and small digital businesses.

WEBSITE	brighousesec.com
EMAIL	sales@brighousesec.com
ENGAGEMENT MODEL	Fixed scope · written authorisation · no passwords required · no call required where suitable
SAMPLE STATUS	Fictional public sample — not client data