uBreach Pro prospecting email templates

Purpose: A partner-ready outreach series MSPs can adapt for existing clients and net-new prospects to position domain exposure monitoring as a practical way to reduce credential-related risk and start stronger security conversations.

How to use these templates

- Tailor the language to the client's industry, maturity, and current security stack.
- Lead with business risk and evidence, not just the dark web as a concept.
- Use one clear call to action in each email, such as a short call, a scan review, or a pilot discussion.
- White-label product references where needed if you do not want to mention usecure by name.

Sequence A: Existing clients

Use this sequence when you want to upgrade current clients with a new exposure monitoring service or add a stronger proof point into reviews, renewals, and expansion conversations.

Email 1: Introduce the risk

Audience: Existing clients

Subject: Find exposed credentials before they become a bigger problem

Hi [First name],

We are reaching out because exposed credentials linked to a business domain can quietly increase the risk of account takeover, social engineering, and follow-on attacks.

Our domain exposure monitoring service helps identify when credentials tied to your domain appear in breach data, so you can respond earlier and with clearer evidence.

This gives you a more proactive view of risk and makes it easier to spot where users, accounts, or processes may need attention before an issue escalates.

If useful, we can walk you through how this works and what the reporting looks like in practice.

Best regards,
[Your name]
[Your company]

CTA: Book a quick walkthrough > [Insert link]

Email 2: Turn exposure into action

Audience: Existing clients

Subject: Why exposed credentials matter more than most teams realise

Hi [First name],

Training, phishing simulations, and policy activity all play an important role. But they do not show whether credentials tied to your domain have already been exposed.

Exposure monitoring adds that missing layer by helping show where users may be more vulnerable to social engineering, where retraining may be needed, and what remediation steps should be prioritised first.

For many clients, this becomes a useful monthly review point because it turns exposure data into something clear, timely, and actionable.

If you would like, we can show you how this could fit into your current security programme and reporting cadence.

Best regards,
[Your name]
[Your company]

CTA: Book a quick walkthrough > [Insert link]

Email 3: Position the upgrade simply

Audience: Existing clients

Subject: A simple way to add domain exposure monitoring into your service

Hi [First name],

One of the easiest ways to introduce this service is to position it as an ongoing visibility layer, not a major project.

Some clients prefer it as a fixed monthly add-on. Others include it in a higher-value security package so it supports broader reporting, review conversations, and proactive recommendations.

Either way, the value is the same: clearer evidence, earlier visibility, and a more practical way to reduce credential-related risk.

If you want, we can recommend the simplest way to package this within your current service model.

Best regards,
[Your name]
[Your company]

CTA: Reply with your current security package and we will suggest a suitable model > [Insert link]

Sequence B: Net-new prospects

Use this sequence when you want to start new business conversations with evidence-led outreach rather than a generic security pitch.

Email 1: Open with relevance

Audience: Net-new prospects

Subject: A simple way to identify credential exposure linked to your domain

Hi [First name],

We work with organisations that want a clearer view of people-related cyber risk without adding more internal admin.

One of the fastest ways to surface that risk is by checking whether credentials linked to a company domain have already been exposed in breach data.

That kind of exposure can make account takeover and social engineering attacks much easier, which is why many businesses now want clearer visibility into it.

If helpful, we can talk you through what this looks like and how ongoing monitoring can support a more proactive security approach.

Best regards,
[Your name]
[Your company]

CTA: Book a quick call > [Insert link]

Email 2: Make the business case

Audience: Net-new prospects

Subject: Why credential exposure is more than a dark web issue

Hi [First name],

Credential exposure is not just a dark web story. It is a business risk issue because exposed credentials can increase the likelihood of phishing-led compromise, account misuse, and preventable security incidents.

That is why we use exposure monitoring as a practical way to start conversations about real risk, not hypothetical risk.

The goal is not just to highlight where exposure exists, but to show what should happen next, whether that is awareness work, tighter controls, or ongoing monitoring.

If this is useful, we can show you how the service works and how other organisations use it as part of a wider security programme.

Best regards,
[Your name]
[Your company]

CTA: Book a quick call > [Insert link]

Email 3: Reduce friction

Audience: Net-new prospects

Subject: A low-effort way to start with exposure monitoring

Hi [First name],

If the main question is effort or return, the easiest starting point is a small pilot or initial monitoring conversation focused on one domain.

This gives you something practical to review without committing to a major rollout, while still creating a clear view of whether credential-related exposure is already present.

From there, we can recommend the most sensible next step, whether that is ongoing monitoring, a broader awareness programme, or a wider human risk discussion.

If you want to explore that approach, we would be happy to talk it through.

Best regards,
[Your name]
[Your company]

CTA: Book a quick call > [Insert link]

Positioning reminder

In partner outreach, do not over-focus on “the dark web” as a concept. The stronger route is to frame uBreach Pro around credential exposure, account takeover risk, social engineering risk, and the value of ongoing monitoring as part of a broader managed security service.