

VELIEDGE



FROM COLD TO GOLD:

# The Ultimate Email Domain Warmup Guide



Bonus: iGaming Spam Words to Avoid



Sanjulian Nis,  
Head of VeliEDGE



# Introduction

Email marketing delivers serious ROI, but here's a catch — only when done right. This is especially critical in iGaming, where operators face stricter scrutiny from email service providers. Skip the warmup process, and you're looking at blacklisted domains, zero deliverability rates, and marketing budgets down the drain.

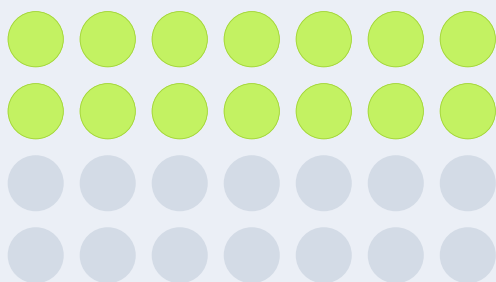
Through our recent expansions in South Africa and Asia, VeliTech has helped iGaming operators worldwide drive results with impactful engagement strategies. As Head of VeliEDGE, I've had a front-row seat to what truly works and what doesn't, and I'm here to share those insights with you.

This guide breaks down the exact warmup process that protects your domain reputation and maximises your email marketing investment. No fluff, no guesswork — just the proven tactics that keep your emails landing where they belong: in your players' inboxes.

# 1 Start small and scale gradually

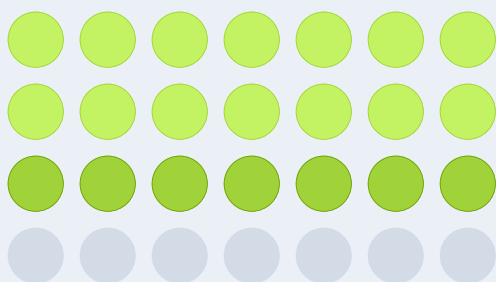
Spikes in email volume or unusual patterns can trigger spam filters. New domains should mimic natural, human-like behaviour, scaling volume as sender authority grows. Use a domain warmup tool to gradually increase your outreach. Here's a sample warm-up plan:

## Days 1–14:



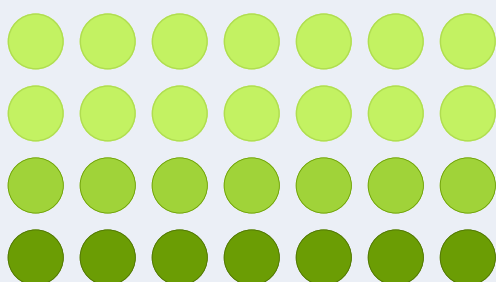
Send a maximum of 50 emails daily to help ESPs see you as safe. Treat your mailbox as a regular business email account by sending authentic messages to trusted contacts, colleagues, or partners.

## Days 15–21:



Slowly introduce automated campaigns for trusted contacts (VIP players, staff members, known affiliates, etc.). Gradually build your daily sending patterns to avoid suspicious spikes.

## Days 22–30:



Continue increasing volume, aiming to reach 40–90 emails a day. Introduce short sending intervals that imitate natural sending behaviours.

Therefore, a proper warm-up of a domain for cold email campaigns and iGaming promotions (5,000+ daily emails) can take up to **two months**. To reduce risks during the warm-up phase, use a separate domain for outreach. This way, if your domain is blocked or flagged, your primary corporate domain (used for your website and communications) will remain unaffected.

## 2 Be consistent and predictable

If you check the domain spam score and find it too high, consistency may be the problem. Try to maintain a sending schedule, with emails dispatched at similar times each day or week. Over time, ESPs interpret regularity as a positive signal.

Consistency helps promotions, too. Anticipate increased activity and incrementally ramp up your sending frequency several weeks in advance, instead of sending rapid-fire in a spike. Finally, scheduling can boost open rates for your players as it builds habitual interactions.

## 3 Keep a delay between emails

ESP algorithms associate rapid emailing with bulk spamming. To protect your email domain spam score, steer clear of huge email volumes per minute. Carefully control delays between emails to mimic human sending, which helps maintain good DR.

It's best to space 40 promotional emails over five hours rather than send them all in a few minutes. Start by leaving around 450 seconds (7 minutes) between emails. Gradually, you can reduce the email frequency to around 67 seconds.

### Days

1-3  
4-7  
8-10  
11-14  
15-20  
21-30

### Delay between the emails

450 sec  
400 sec  
250-300 sec  
200 sec  
100 sec  
>67 sec



## 4 Keep emails short

Both players and ESPs prefer shorter emails that get to the point. Make sure you clearly state the offer's benefit or purpose within the first two lines. In my experience, around **50 words** in total are enough to capture attention and avoid spam filters. Regularly test email length against key engagement metrics. Compare shorter and slightly longer messages to find what works with your players.

## 5 Use real email addresses for warmup

To maintain a high sender reputation, email marketing managers should use only valid and active addresses. But how do you know which ones are safe to use?

Email addresses fall into three categories:

### VALID

address is safe, verified, and ideal for warmups and sequences

### RISKY

address exists but poses a higher bounce risk due to disposable domains, catch-all setups, or potential spam traps

### INVALID

address has syntax errors, DNS issues, or a full mailbox

Regular list maintenance not only protects your domain reputation but also optimises your email marketing budget by removing recipients who never open, click, or reply. Use tools like ZeroBounce or EmailListVerify to regularly clean your lists, identify abandoned inboxes, and correct typos. At the same time, beware of automated tools that rely on fake addresses just to boost volume. As a rule of thumb, keep risky addresses to **no more than 20%** of your list.

For new domains, you can start with a pre-warmup by sending emails to colleagues or trusted contacts. ESPs interpret their natural opens, clicks, and replies as early positive signals.

## 6 Set clear performance benchmarks

Concrete performance indicators help you understand how to warm up email domains effectively and detect early signs of reputation loss. How to reduce risks during the warmup phase? Aim for an 80% open rate, a bounce rate below 5%, and a spam complaint rate of less than 0.05%. To achieve these targets, use highly engaged recipients for your first communications.

### Initial Success Indicators

80%  
open rate



< 5%  
bounce rate



< 0.05%  
spam complaint rate



## 7 Avoid poor writing practices

Avoid fluff and attention-grabbing language like “Free Money,” “100% Guaranteed,” or “Claim instantly”, which are common triggers for anti-spam tools. The same goes for excessive capitalisation and punctuation (for instance, multiple exclamation marks, dollar signs, or emojis in subject lines). Be careful with the entire body of the email, and not just the text. Modern spam filters with OCR (Optical Character Recognition) ability can detect suspicious words even in images.

To save you the trouble, our team prepared a list of iGaming spam trigger words that could hurt your deliverability.

# iGaming Spam Words to Avoid

## 1. Financial Promises & Gambling-Related Triggers

These words are commonly associated with high-risk financial activities, gambling, and promises of wealth, making them highly spam-sensitive in iGaming.

- Winnings
- Lottery
- Double money
- Jackpot
- Prize
- Make money
- Casino
- Payout
- Instant cash
- Cash prize
- Big win
- Risk-free
- Cash bonus
- No risk
- Get paid
- Gamble
- Easy money

## 3. Payment-Related Triggers

These words are linked to online transactions, which can raise security concerns in email filters.

- Deposit
- Withdraw
- Payout
- Wire transfer
- Bank transfer
- PayPal
- Cryptocurrency
- No credit card required
- Instant payout
- Instant withdrawal
- Full refund

## 5. High-Engagement & Clickbait Triggers

These words encourage user interaction but might also be flagged as misleading.

- Click here
- Open now
- Instant access
- See for yourself
- Get started today
- Your chance to win

## 2. Urgency-Based Triggers

These words signal aggressive sales tactics or misleading urgency, which email filters often flag.

- Act now
- Don't miss out
- Exclusive deal
- Limited time
- Urgent
- Hurry
- Offer expires
- Once in a lifetime
- Special promotion
- Sign up now
- Join for free
- 100% free

## 4. Too-Good-to-Be-True Triggers

These words raise red flags due to their frequent association with scams.

- Guaranteed
- Promise you
- No strings attached
- No catch
- Winner
- Claim your prize
- You have been selected
- Your account has been credited
- Exclusive access
- Giveaway

## 6. Legal & Compliance-Related Triggers

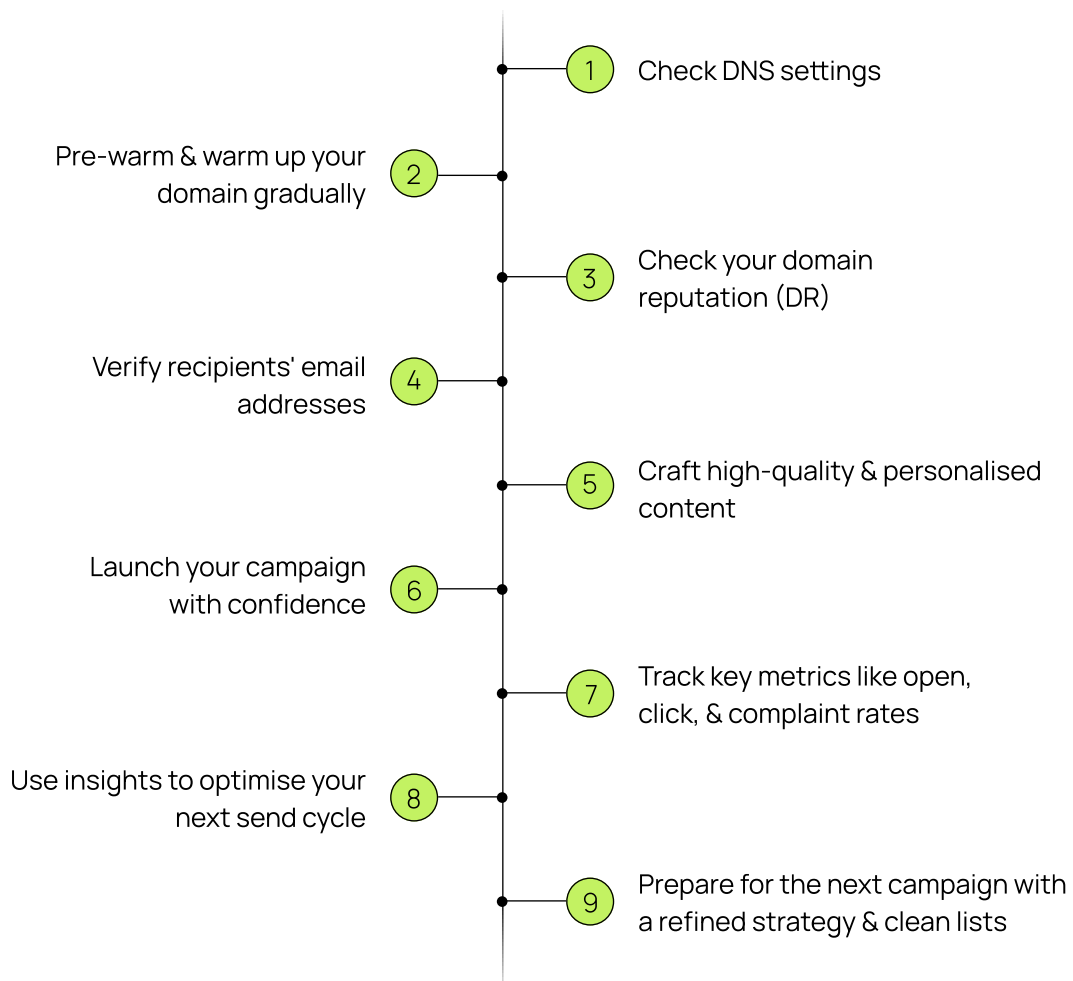
These terms can be flagged due to potential legal implications.

- 100% legal
- No obligation
- Certified
- Risk-free investment
- No risk guarantee
- Legal approval

# Key takeaways?

- Avoid overuse of iGaming spam trigger words, especially in subject lines.
- Write in a natural, conversational tone rather than using clickbait.
- Personalise emails.
- Balance text and images — emails with too many images and little text often get flagged.
- Ensure sender credibility by using a verified domain and proper SPF/DKIM authentication.

But getting your domain warmed up is just your first move. To land in inboxes instead of spam folders, follow this proven flow for high-impact campaigns:



This approach isn't theory — it's battle-tested. During our cooperation with **BlueChip**, the client used it to break through the noise and dominate one of the toughest iGaming markets: India. Truth is, it wasn't just email tricks — it was a full-scale omnichannel strategy powered by VeliEDGE. Check out the before vs. after to see the impact.

## VELIEDGE

### Before

### After



**Limited workflow capabilities** with additional costs for scaling



**200+ active workflows** — zero extra fees



**Higher costs** due to third-party integrations



**No extra costs:** all tools included within the platform



**One-size-fits-all solutions** with minimal collaboration



**Boutique-like service** with regular syncs and continuous optimisation

Over time, our partnership with BlueChip evolved into full ecosystem adoption, helping the client become one of the region's rising stars — with exceptional growth across the board:

**4.5M**

in-app messages sent via VeliEDGE CRM

**18M+**

bets processed every month

**20%**

uplift in player LTV

**20K+**

new players acquired monthly

**12K+**

games live on BlueChip

**15+**

tournaments hosted monthly

**\$400K+**

in crypto bets processed

[Discover the full success story](#)



# ML-Driven Ecosystem For iGaming Operators

From the buzz of African betting shops to the glamour of European casinos, our product suite drives up to 8x GGR growth and a 15% DAU boost for iGaming brands.



Trusted by:



Power your next big win with  
**VELITECH**

[Contact us](#)