



# PENETRATION TESTING CAMPAIGN

CONTENT ASSETS

# EMAIL TEMPLATES

## ATTRACT YOUR CUSTOMERS AND CREATE NEW LEADS

---



Use these emails individually or as a nurturing sequence, complete with your own call-to-action.

### EMAIL 1

#### RAISE AWARENESS OF THE VALUE OF PENETRATION TESTING

Subject: Now's the time to find your security weaknesses

Hi <Name>,

With many companies now operating entirely remotely, we've seen an increase in security misconfigurations as a result of rushed implementations of cloud-based technologies and new processes. In fact, 32% of critical vulnerabilities are caused by outdated components.

Regular penetration testing is therefore more vital than it has ever been. By booking a penetration test with <Partner Name>, you can identify your unknown vulnerabilities and get detailed advice on the remediation steps needed to avoid an attack.

We work with industry-leading penetration testing specialists to ensure you get the maximum benefit from your test, which will offer:

- **Thorough testing of all apps and systems**  
Benefit from increased cyber security right across your infrastructure, as every component can be tested, including network, systems, apps and even people (via social engineering).
- **Clear remediation plan**  
Quickly understand your vulnerabilities and the steps you need to take to fix them. Our comprehensive remediation reports combine a high-level executive summary with a detailed technical breakdown.
- **Affordable expertise**  
Expert penetration testing is now accessible to organisations of all sizes thanks to flexible, affordable packages.
- **Proven track record**  
Our partner Bulletproof has a proven track record in finding all types of cyber weaknesses, with 1,000s of tests performed across all industry sectors.

<Partner sign off and CTA>

## EMAIL 2

### FOLLOW UP & PROVIDE DEEPER INSIGHT WITH A CO-BRANDED INFOGRAPHIC

Subject: Secure your data with a penetration test

Hi <Name>,

Cyber attacks are on the rise – our trusted cyber security partner Bulletproof saw a 350% rise in phishing attacks in a single quarter last year. It's more vital than ever that organisations find and fix security weaknesses before a hacker exposes them. Penetration tests are the most effective way to uncover vulnerabilities, which is why regular pen testing is also mandated by standards such as PCI DSS and ISO 27001.

#### **Why use <Partner X> for your penetration test?**

We partner with trusted cyber security partner Bulletproof, who only use CREST-certified and Tigerscheme approved testers, to ensure you get an expert security assessment. We offer a variety of test types to target and test all aspects of your security process:

- Network & infrastructure testing
- Web application testing
- Mobile application testing
- Social Engineering prevention services
- Red Team security testing

[OPTIONAL] We have created an infographic <link to co-branded 'Key Insights' infographic'> highlighting the most common security flaws to help you understand how penetration testing can enhance your cyber security strategy.

<Partner sign off and CTA>

## EMAIL 3

# INCREASE CUSTOMER ENGAGEMENT AND USE OUR WHITEPAPER TO CAPTURE LEADS

Subject: Get penetration testing right for your business

Hi <Name>,

Protection from hackers is a priority for businesses looking to secure remote working and maintain their compliance with legal and regulatory standards. Penetration testing services are a fundamental component of a good risk management programme, but not knowing the ins and outs of how they work can make it hard to get the best value from your test.

We've worked with our trusted penetration test partner Bulletproof to put together this guide <link to security first whitepaper>. Download your copy today <link to landing page> to find out:

- Why penetration test is key to a solid cyber security strategy
- How to choose the right test to meet your business objectives
- How to plan and manage penetration tests effectively

Through our partnership with Bulletproof, we are confident we can offer you effective testing with a fast turnaround, allowing you to quickly deal with any vulnerabilities discovered. Our penetration tests are competitively priced and come with easy-to-understand reports containing clear remediation advice.

We strongly recommend penetration testing as an effective way to identify and remediate your security vulnerabilities. <Partner CTA>

<Partner sign off>

# SOCIAL MEDIA COPY CAPTURE YOUR AUDIENCE'S ATTENTION WITH TRIED AND TESTED TOPICS



These examples are based on our top-performing social posts and can be used as they are or adapted to fit your company's tone of voice.

## LinkedIn

Why should you book regular penetration tests? Our partner Bulletproof found that, in 2020, 1 in 4 tests revealed a critical security flaw with unpatched components still the top vulnerability for companies. Our infographic reveals more about the scale of the issue and how penetration testing helps keep your critical business data safe. #cybersecurity #penetrationtests <link to infographic>

To meet industry best practice and #compliance standards, #penetrationtests should be conducted at least once a year. Our trusted cyber security partner Bulletproof found that a quarter of their customers fell into the critical – high vulnerability category, an increase on previous years. To stay ahead of the hackers and prevent business-damaging breaches, contact <PARTNER CTA TO BOOK PEN TEST>

## Twitter

One of the best ways to avoid a #cyberattack is to identify and remediate your organisation's vulnerabilities with a penetration test before a hacker finds them. To book <CTA>

It's best practice to perform a #pentest at least once annually to stay on top of new vulnerabilities. Give us a call on <partner phone number> and ensure your business stays protected in 2021

#Penetrationtests are a great way to stay ahead of #hackers. By uncovering security flaws in your apps and infrastructure, you can address any weaknesses before a hacker exploits them. Discover key insights with our #pentest infographic: <link to co-branded infographic>

It's important to understand your #penetration test to get the best outcomes for your business security. This guide from our partner @bulletproofsec takes you through everything you need to know: <link to whitepaper landing page>

# BLOG ARTICLE OUTLINES

## SHARE ADVICE AND BEST PRACTICE WITH YOUR CUSTOMERS

---



To avoid content duplication and improve SEO outcomes, we've provided suggested article outlines that you can work up in your own corporate tone of voice and place on a blog, in a newsletter or wherever most appropriate. These outlines can also be used to brief external content creators. Use either or both to complement the other content in your penetration testing campaign.

### ARTICLE ONE

*To raise awareness of the importance of penetration testing and how it fits into a well-rounded cyber security strategy. Target: IT Decision maker, SME – not security specialist but responsible for procurement of security services.*

#### **Suggested Title: Why penetration testing should always be high on your security agenda**

Introduction: What is a penetration test?

- Penetration testing is a technical exercise involving active and passive analysis of IT infrastructures and applications for security vulnerabilities
- Conducted by a third-party expert at an arranged time, to a pre-defined scope
- Sometimes also includes testing the 'human element' – your employees – through social engineering
- Also known as ethical hacking or 'white hat' hacking

Takeaway 1: How does it fit into your strategy?

- Identifies shortcomings in the confidentiality, integrity and availability of data.
- Provides risk analysis of the impact of discovered vulnerabilities, and remediation advice
- Allows those responsible for cyber security to prioritise, plan, budget and remediate in a methodical way

Takeaway 2: Cyber attacks are on the rise

- Attacks are on the rise, with 86% of UK organisations expecting attacks to increase significantly this year
- In 2020, Bulletproof found 1 in 4 penetration tests revealed a critical flaw
- 'Socially engineered' attack types such as phishing have seen a significant increase, in part due to the shift to remote working



### Takeaway 3: Remote working

- Remote working is not going away – many businesses post pandemic are considering a hybrid or all-remote model
- Securing your remote workforce – time now to evaluate the measures put in place in 2020 and ensure your data is protected without compromising team's ability to do their work (Gartner)
- Penetration testing helps you find your flaws before a hacker can exploit them

### Takeaway 4: Compliance and data protection

- Penetration testing isn't just part of 'best- practice' – it's included in a wide variety of compliance standards
- Regulations including PCI-DSS, ISO 27001 and FCA stipulate that you should or must have regular tests
- Tests can be tailored to meet the requirements you need to maintain adherence to your industry's compliance regulation
- It also helps you demonstrate that you meet the GDPR's requirement to have a process in place for *“regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of [data] processing”* (Article 32)

### Conclusion

- Organisations large and small should add penetration testing to their security practices to fully protect themselves against cyber attack
- Regular testing helps you build a cycle of continuous feedback and improvement as part of a true security culture
- It can also help you attain and maintain compliance with key industry standards
- Call to Action (CTA)
  - CTA could include link to whitepaper landing page 'learn more'
  - CTA could also include a direction 'contact to book'

### Supporting links and resources:

Recent Bulletproof blog:

<https://www.bulletproof.co.uk/blog/5-reasons-you-need-to-pen-test-in-2021>

Co-branded whitepaper “Security First: an Essential Guide to penetration testing”

Co-branded Infographic “Key Insights in Penetration Testing”

Gartner: “Top Security projects for 2020/2021”

<https://www.gartner.com/smarterwithgartner/gartner-top-security-projects-for-2020-2021>

## ARTICLE TWO

*To help interested customer prospects understand the type of penetration test they need and demonstrate the partner's expertise and range of services available. Target: IT Decision maker, SME – not security specialist but responsible for procurement of security services*

### **Suggested Title: Picking the right penetration test for your business**

Introduction: What is a pen test:

- Penetration testing is a technical exercise involving active and passive analysis of IT infrastructures and applications for security vulnerabilities
- Conducted by a third-party expert at an arranged time, to a pre-defined scope
- Sometimes also includes testing the 'human element' – your employees – through social engineering
- Also known as ethical hacking or 'white hat' hacking

Takeaway 1 – What types of penetration test are there?

- It's important to discuss the type of test you are ordering to ensure you are targeting the appropriate aspect of your security process
- Infrastructure or network testing - assessing infrastructure or a network for its current operational security levels, such as running services, current patch levels, improper configurations, flaws in design and effectiveness of security controls.
- Application testing – testing the functionality, process flow and security controls of an application (including mobile and web) to discover any interactions that could create security issues
- Social engineering prevention services – testing your employees' security vigilance by simulating a targeted attack by malicious hackers
- 'Red Team' testing – designed to simulate a real-world attack, a detailed security assessment that attempts to break every layer of your physical and cyber security defences.

Takeaway 2 – What approach should you take?

- Three main approaches: black box, white box and grey box
- Black box – a realistic scenario, sometimes called a 'controlled hack'. Very little information is given to the penetration testing company, putting them in a similar situation as a real-world hacker. This can mean though that not all areas of your target infrastructure get tested, as they may not be discovered
- Grey box – partial information about the target systems is given to your testers. This could include basic user level access, giving a chance to explore the internal systems
- White box testing – the most thorough test, where full details of the target's internal infrastructure, how it works and the levels of access are shared with the test company. This 'full disclosure' does not give a realistic simulation of an attack but does provide a more comprehensive view of security issues, often in a shorter timeframe.



#### Takeaway 4 – Picking a reputable pen test partner

- You will need to find a partner who has both the trusted reputation to be given access to your systems, with the right technical skills to do the job well
- A reputable company will help you choose the right type of test and approach to meet your security objectives, and provide you with an easy-to-read report detailing any uncovered risks
- Look out for certification from industry bodies like Tigerscheme and CREST to give confidence your partner is competent and trustworthy

#### Results/conclusion

- Penetration tests are an important part of a well-managed cyber security strategy
- It's important for IT decision makers to understand the different types and options of test in order to meet their objectives and to obtain meaningful results
- Call-to-action (CTA):
  - CTA could link to whitepaper “To understand how to choose, scope and prepare for your penetration test...”
  - CTA could link to infographic “The most common recent security flaws to inform your cyber security strategy”
  - CTA could also include a direction ‘contact to book’

#### Supporting resources:

Co-branded whitepaper “Security First: an Essential Guide to Penetration Testing”

Co-branded Infographic “Key Insights in Penetration Testing”

Bulletproof website: <https://www.bulletproof.co.uk/penetration-testing>

CREST Pen Test Procurement Guide:

<https://www.crest-approved.org/wp-content/uploads/PenTest-Procurement-Guide.pdf>

# LANDING PAGE CONVERT INTEREST INTO LEADS FOR YOUR SALES TEAM



If appropriate, you could create a landing page to convert visitors to your own website into leads. This could include the co-branded whitepaper 'Security First' or alternatively any new content assets or web events you choose to create to build out your campaign.

## Headline : Everything you need to know about booking and scoping your penetration test

Penetration testing, or pen tests, can be a confusing subject for many businesses. What actually is a penetration test? Why do you need one? How can they help?

This Security First whitepaper goes through everything you need to know to make an informed decision when booking and scoping a penetration test. The report contains:

- An in-depth explanation of penetration testing
- Clarity on the difference between unauthenticated and authenticated tests
- The difference between an application test and an infrastructure test
- Introduction to social engineering
- Scoping information
- Security standards

Schedule your next penetration test with confidence.

CTA Button "Get your free guide today"

*This should be accompanied by an image of the co-branded cover of the whitepaper.*



