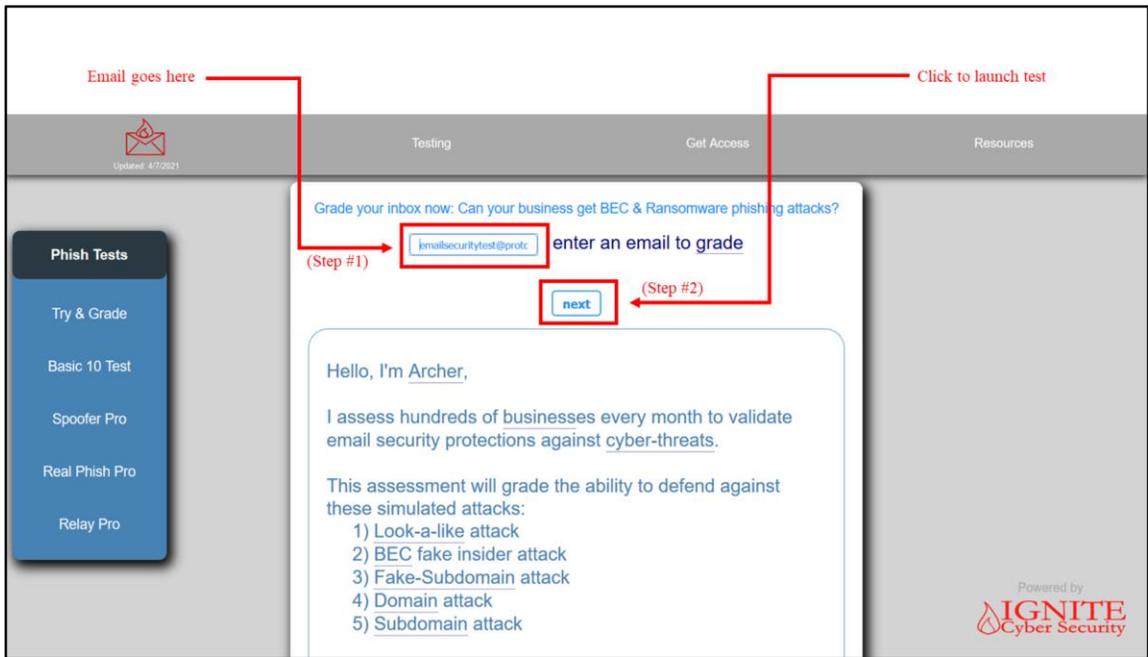


In this video I'll show how to use EmailSpooftest.com to grade a domain's ability to defend against email based cyber attacks. To begin, navigate to EmailSpooftest.com as I have done here.



First, enter any email address you have access to, these tests work on all mail systems. Then, click the button labeled “next” to launch the test.

Scroll down to get to the score card

Check your inbox

testing public mail system: protonmail.com (Target Email tests are sent to) (Test ID)

10 test emails were sent to emailsecuritytest@protonmail.com with ID: 6503 in the subject. It could take up to 5 minutes for delivery.

Look in emailsecuritytest@protonmail.com's inbox, junk folders, and mail logs to see if emails numberd E1-E10 were received or rejected.

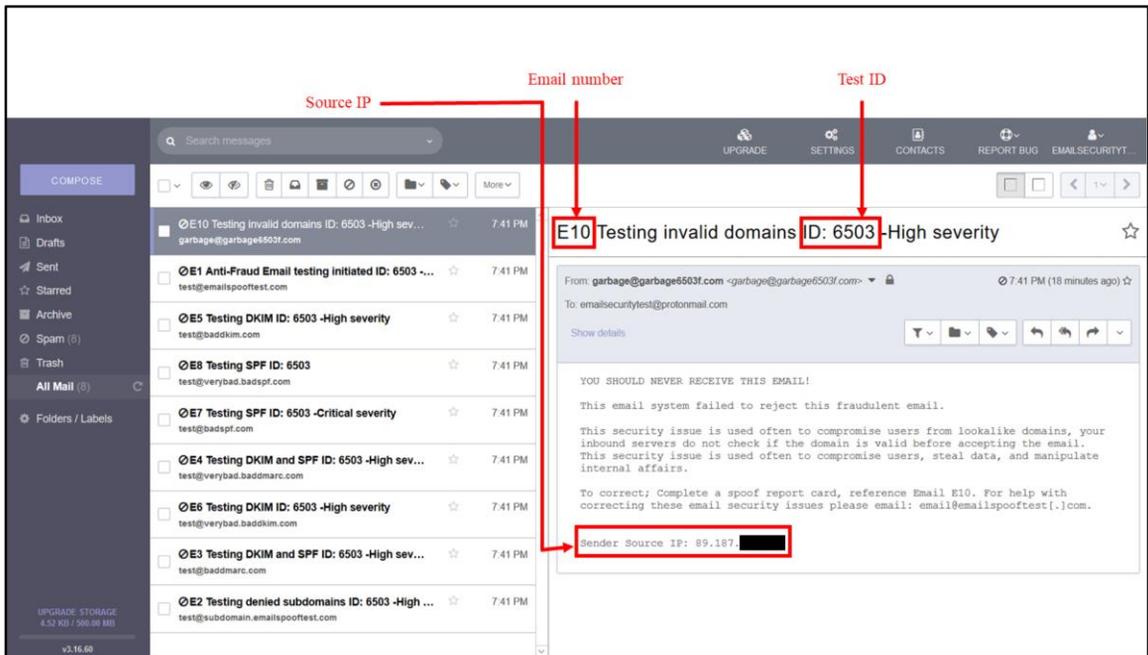
To grade your basic 10 email security controls, fill in the test results card below.

**To grade your results and pinpoint issues complete this form;**  
 search emailsecuritytest@protonmail.com inbox, junk/ spam folders, and mail logs for test ID: 6503 to complete the testing results

Email tests (E1-E10)	Did you get the email?	Technical Results
E1:	<input type="radio"/> Junk <input type="radio"/> Inbox <input type="radio"/> Undelivered <input type="radio"/> Not	-- Make a selection then click [Grade Results] below to see results here

Powered by

The page will update with your testing ID, and the target email the tests were sent to. In the next steps I scroll down to complete a scorecard.



Next, check the inbox the tests were sent to and fill out the scorecard accordingly. Find emails E1-E10 in your inbox or junk. If you didn't receive an email after 5 minutes, then mark that email undelivered. Undelivered emails should be validated in the email server logs.

Looking at my inbox, I have one of the test emails open. In the subject is the test number and the testing ID. The body of the email will contain some information about the test, why it's bad, and an email to reach out for help. The body will also contain the source IP from which the test was initiated.

My inbox received emails 1, 2, 3, 4, 5, 6, 7, 8, and 10 in spam and email 9 was undelivered. Now, I go back to emailspooftest.com and enter the results into the scorecard.

(Step #3) Complete scorecard

(Step #4) Click to get grade

Testing	Get Access	Resources
<b>Email tests (E1-E10)</b>	<b>Did you get the email?</b>	<b>Technical Results</b>
E1:	<input checked="" type="radio"/> Junk <input type="radio"/> Inbox <input type="radio"/> Undelivered	— Make a selection then click [Grade Results] below to see results here
E2:	<input checked="" type="radio"/> Junk <input type="radio"/> Inbox <input type="radio"/> Undelivered	— Make a selection
E3:	<input checked="" type="radio"/> Junk <input type="radio"/> Inbox <input type="radio"/> Undelivered	— Make a selection
E4:	<input checked="" type="radio"/> Junk <input type="radio"/> Inbox <input type="radio"/> Undelivered	— Make a selection
E5:	<input checked="" type="radio"/> Junk <input type="radio"/> Inbox <input type="radio"/> Undelivered	— Make a selection
E6:	<input checked="" type="radio"/> Junk <input type="radio"/> Inbox <input type="radio"/> Undelivered	— Make a selection
E7:	<input checked="" type="radio"/> Junk <input type="radio"/> Inbox <input type="radio"/> Undelivered	— Make a selection
E8:	<input checked="" type="radio"/> Junk <input type="radio"/> Inbox <input type="radio"/> Undelivered	— Make a selection
E9:	<input type="radio"/> Junk <input type="radio"/> Inbox <input checked="" type="radio"/> Undelivered	— Make a selection
E10:	<input checked="" type="radio"/> Junk <input type="radio"/> Inbox <input type="radio"/> Undelivered	— Make a selection
		<a href="#">Grade results</a>

Powered by **IGNITE** Cyber Security

When complete, click the “Grade results” button at the bottom.

The screenshot displays the 'Email Security Grades for protonmail.com' interface. On the left, a sidebar lists various testing options: 'Phish Tests', 'Try & Grade', 'Basic 10 Test', 'Spoof Pro', 'Real Phish Pro', and 'Relay Pro'. The main content area shows a table of test results with columns for test type, status, and grade. A red box highlights the date and time of the test: '4/7/2021 1:21:46 PM'. Another red box highlights the target email address: 'emailsecuritytest@protonmail.com'. At the bottom, there are two buttons: 'Email grades to emailsecuritytest@protonmail.com' and 'New Test'. The interface is powered by 'IGNITE Cyber Security'.

Test	(ID)	(Source IP)	Grade	Notes
Control test - valid email -			Grade: A	Notes:
Fake subdomain protection -			Grade: D	Notes:
BEC fake insider protection - Enforced:			Grade: A	Notes:
Look-a-like protection -			Grade: F	Notes:
Domain attack protection -			Grade: D	Notes:
Subdomain attack protection -			Grade: D	Notes:

The screen will update with the grades for the email domain tested, as well as testing details.

Below you can email the graded results to the email address used in the test, along with a button labeled "New Test" which can be used to start a new testing session.

From my testing shown in this tutorial, I can see that the email domain I tested received an A for the control test and the BEC fake insider test but the domain is vulnerable to Fake subdomain attacks, look-a-like attacks, domain attacks, and subdomain attacks.

# Advanced access

Email tests (E1-E10)	Did you get the email?	Technical Results
E1 valid email (test control)	<input type="radio"/> Junk <input checked="" type="radio"/> Inbox <input type="radio"/> Undelivered	<p><b>Pass</b></p> <p>You are able to receive valid emails from domains normally. This means we will get the most accurate testing results possible.</p>
E2 disabled subdomain test	<input type="radio"/> Junk <input checked="" type="radio"/> Inbox <input type="radio"/> Undelivered	<p><b>Fail</b></p> <p>Subdomains of the sending domain (exampletest.com) are specifically blocked in DMARC system did not protect against DMARC subdomain fraud for DMARC aligned domains.</p> <p>Fix: set inbound email servers to check DMARC for subdomain enforcement</p> <p>ExampleTest.com DNS settings</p> <p>DMARC - Quarantine (Report SPF   Enforce DKIM  &gt;DMARC1_p=quarantine;fo=1;policy=reject)</p> <p>SPF - Allow MX, deny others (except the include subdomain test -all)</p> <p>DKIM - email not signed (selector = s1  &gt;DKIM1;v=1;g=2011 )</p>
E3 strict DMARC reject all	<input type="radio"/> Junk <input checked="" type="radio"/> Inbox <input type="radio"/> Undelivered	<p><b>Pass</b></p> <p>System enforces strict DMARC connection security</p>
E4 strict DMARC reject all, reject subdomains	<input type="radio"/> Junk <input checked="" type="radio"/> Inbox <input type="radio"/> Undelivered	<p><b>Pass</b></p> <p>System enforces strict DMARC connection security</p>
E5 strict DKIM alignment	<input type="radio"/> Junk <input checked="" type="radio"/> Inbox <input type="radio"/> Undelivered	<p><b>Pass</b></p> <p>System enforces strict DKIM controls</p>
E6 strict DKIM alignment, reject subdomains	<input type="radio"/> Junk <input checked="" type="radio"/> Inbox <input type="radio"/> Undelivered	<p><b>Pass</b></p> <p>System enforces strict DKIM subdomain controls</p>
E7 SPF reject all	<input type="radio"/> Junk <input checked="" type="radio"/> Inbox <input type="radio"/> Undelivered	<p><b>Pass</b></p> <p>System enforces SPF controls</p>
E8 SPF reject all, reject subdomains	<input type="radio"/> Junk <input checked="" type="radio"/> Inbox <input type="radio"/> Undelivered	<p><b>Pass</b></p> <p>System enforces SPF subdomain controls</p>
E9 internal authentication	<input type="radio"/> Junk <input checked="" type="radio"/> Inbox <input type="radio"/> Undelivered	<p><b>Pass</b></p> <p>System rejects spoofed internal emails</p>
E10 reverse DNS	<input type="radio"/> Junk <input checked="" type="radio"/> Inbox <input type="radio"/> Undelivered	<p><b>Pass</b></p> <p>System rejects invalid domains</p>

Advanced access users get additional troubleshooting data as well as unlimited access to email testing tools to fix and tune email security systems. To get advanced access click on the “Get Access” link on [emailspooftest.com](https://emailspooftest.com)