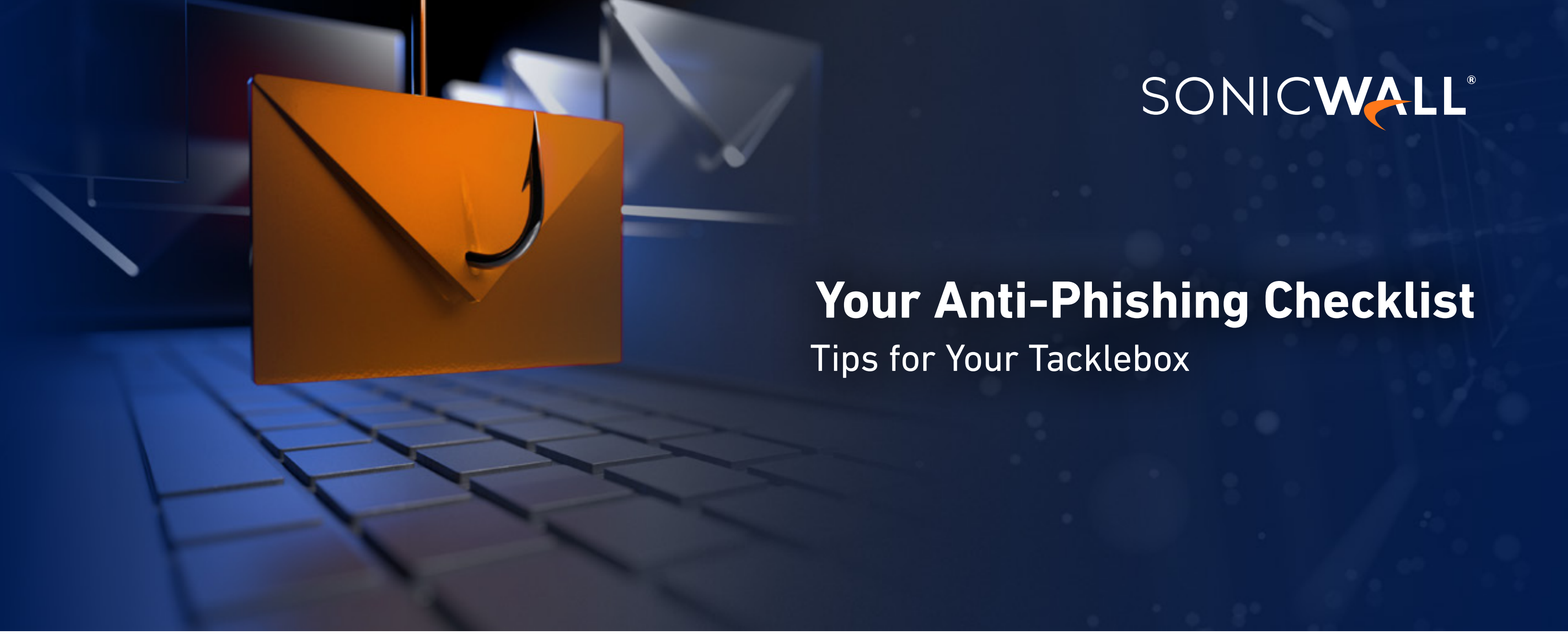

SONICWALL®

Your Anti-Phishing Checklist

Tips for Your Tacklebox

Introduction

Cloud computing has impacted everything from business operations to how we interact with one another. But all that convenience comes with added vulnerability, and every connection creates new opportunities for hackers. This checklist is designed to serve as a guide so you can stay ahead of threat actors. It will provide you with valuable insights and actionable takeaways to better protect your organization from phishing attacks.

Invest in Tools That You Invest In

Cybersecurity tools can be complex. By taking time to understand exactly what a tool can do, it can help you to maximize the investment already made. Not only can it save you the additional cost of purchasing another tool, but it can also optimize your efficiency by having fewer screens to manage. Additionally, you may discover that you already own a solution to a minor problem that you may not get funding for.

Use a Strong Passphrase, Not a “Password”

With the increasing power of computers, cracking a password of eight alpha characters can take less than five minutes; A password with eight alphanumeric and special characters only adds three hours of computational time to crack. However, if we use passphrases of only the uppercase and lowercase characters to make a passphrase of the first six words of a song or a book, the estimated time to crack becomes centuries with today’s current processing power. Wouldn’t you rather remember ‘FlyEaglesFlyOnTheRoad’ vs ‘ZrX{5)ud’?

Activate MFA

Multi-factor authentication (MFA) requires that users use two or more pieces of evidence (factors) to ensure that the user is authorized to access a system and that the user is who they claim to be. The factors should come from different categories: something that you *know*, something that you *have* and something that you *are*.

Check the Sender’s Address Before Interacting

Many times, emails that claim that they come from a well-known organization will use their logos to help with the apparent legitimacy of the email. Many scam emails do a poor job of emulating all the details of a legitimate email. One of the more challenging aspects of such an email is the sender’s email address. Often the attackers use free email services such as Gmail or Yahoo to send their emails. In some cases, they may register random domains that aren’t affiliated with the impersonated organization. Finally, if the address is looked at closely, you may see that the domain name is a look-alike that swaps the letters ‘I’ and ‘L’ or replaces the letter ‘O’ with a ‘zero’.

Pay Attention to Grammar Mistakes, But Don’t Stop There

Historically, phishing and scam emails have had poorly constructed messages, often with phrases not normally heard in conversational English. Emails with excessive grammatical errors should be a red flag for malicious emails. However, with the development of natural language artificial intelligence (AI), threat actors are now able to turn poorly worded emails into emails that could have been written by an English major.

Be Wary of All Hyperlinks and Attachments

Emails with attachments or links are more difficult to process by email sanitation tools and are often used by threat actors to circumvent security.

Conduct Health Checks

Having your security posture or configuration evaluated by either a third party of the manufacturer or a consultant can provide valuable insight into how you are using the tools you've deployed.

Modernize Legacy Tech

A key attack vector of threat actors is exploiting patched vulnerabilities. These unpatched vulnerabilities may be zero-day threats that were just identified or part of an end-of-life appliance that is no longer covered by a maintenance/support agreement.

Conclusion

More than 90% of today's data breaches start with a phishing attack. By using this checklist, you're on your way to better protection for your organization.

While you're here, try out our Phishing Quiz! It uses real-world examples to help determine your "phishing IQ." In this quick quiz, you'll get to read through a series of emails and determine which emails are real and which emails are bait. Try it now!

Receive actionable cost and usage optimization recommendations that you can implement and automate with the click of a button
Receive actionable cost and usage optimization recommendations that you can implement and automate with the click of a button
Receive actionable cost and usage optimization recommendations that you can implement and automate with the click of a button

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non- infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profits, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.