WHITE PAPER

Recommendations for Successful Security Awareness Programs

Introduction

Security awareness training, when done right, dramatically improves your security posture, keeping employees vigilant to the constant threat of scams and other attacks that prey on human error. With the major disruption to work routines and the acceleration of phishing activity caused by COVID-19, the need for effective, accountable and relevant training has never been greater. But there is a problem. Training is outside the skillset for most IT admins, and the level of effort to set up and run a program of training courses, compliance accreditations and phishing simulations can be daunting.

This short white paper provides recommendations on how to avoid the pitfalls of starting your organization's security training journey, helping you to maximize the impact of your efforts.

1. Get buy-in from stakeholders

You may already have a security perimeter that includes endpoint protection, DNS or web filtering and anti-spam, but the primary tactics used in successful cybersecurity breaches are phishing and social engineering.[1] Ensuring that your stakeholders understand these threats is the first step to initiating and then running a successful security awareness program.

Send an email introducing the program to management. Explain the importance of educating users and measuring and mitigating your risk of exposure to phishing and other social engineering attacks. Be sure to share details around your first phishing and training campaigns. If applicable, loop in your local IT support so they are aware of the program and training schedule.

2. Allow the IP address for Webroot's mail server

To prevent problems related to training or simulated phishing email delivery, you need to configure your mail server to trust Webroot's IP address for email sends: 167.89.85.54. See our detailed guides on how to do this for Microsoft® Exchange and Microsoft® 365, and for G Suite Gmail.

3. Import users via Microsoft® Azure AD

To simplify enrollment and ongoing user management, Webroot provides a SCIM-based Microsoft Azure Active Directory (AD) integration. This makes it easy for any organization subscribed to Microsoft 365 to import users without the setup and costs imposed by other Azure AD integration models. The Webroot Azure AD integration:

- Doesn't require any alterations to your Azure AD subscription
- Doesn't require any infrastructure or agents to be deployed on-premises
- Doesn't require Azure-hosted LDAP-dependent provisioning services
- Is deployed more rapidly with substantially lower onboarding costs

The Azure AD integration keeps users in the Security Awareness Training console in sync with the AD tenant, so you don't need to upload CSV or LDIF files or manually create users (although these options are available, if you require or prefer them). This helps automate the initial import of target users, as well as the future adding/removing of users as they join or leave the organization. From the Microsoft Azure portal, you can choose to sync all users or only specified AD groups who require training.

To set this up, open the Webroot management console. Go to Settings > Security Awareness Training and click **Configure Azure AD Integration**. From there, you can obtain the secret token and get more detailed instructions on how to use Microsoft Azure AD.

Note: Users can always be imported via Azure AD, Active Directory LDIF file, CSV file or a web-based form. Tags allow easy grouping of users by location, department or category to help you target your campaigns.

4. Start with a baseline phishing campaign

When you run your first phishing campaign, you establish your starting point for measuring and demonstrating improvement over time. Ideally this initial campaign should be sent to all users without any type of forewarning or formal announcement (except to any stakeholders who signed off on the program; though they should be tested too). Use the **Broken Link** option when choosing a landing page for the campaign so you don't alert users they are being trained.

Recommended Phishing Templates:

- Account Reset
- COVID New Company Policy: Communicable Disease Management Policy

5. Set up essential security training

Create training campaigns to cover essential cybersecurity topics including phishing, social engineering, passwords and more. The Webroot Cybersecurity Essentials series provides a good overview.

Recommended Training Courses:

- Phishing – Understanding Phishing
- Email – Cybersecurity Essentials
- Passwords – Cybersecurity Essentials
- Remote Work – Stay Cyber Resilient While WFH

6. Launch appropriate compliance training

Create training campaigns with compliance courses appropriate for your organization and the employees who need them.

Recommended Training Courses:

- GDPR – A Regulated Ruse
- CCPA – Fired Up About CCPA
- HIPAA – An Avoidable Accident
- PCI – The Disinterested CEO

7. Establish monthly phishing simulations

Measure the success of your program and keep an eye on high-risk users by running regular phishing simulations. If you can't run phishing simulations monthly, strive for a quarterly cadence. If you get pushback on sending emails to everyone, then prioritize testing users who failed the previous round.

8. Set up monthly training

Security awareness programs are most successful when run continuously and sustained over the long term, instead of treated as a one-off annual requirement. Regular engagement with employees reminds them to stay vigilant. Using our shorter 4-5-minute modules in between more substantial training is an effective tactic to keep security top of mind while avoiding user fatigue. Below is a list of recommended training modules to consider over a period of 18 months:

#	Training Module
1	Spear Phishing – A Terminal Mistake
2	Phishing – Understanding Phishing, Full Length
3	Charity Scams – Charity Case
4	Remote Work – Stay Cyber Resilient while WFH
5	Cybersecurity – Understanding Cybersecurity
6	Breach Awareness – Introduction
7	Email Attachments – Scams Gone Viral
8	Malware – Understanding Malware
9	Physical Security – Let's Get Physical
10	Physical Security – Cybersecurity Essentials
11	Social Engineering
12	Passwords – Your Page is My Page
13	Passwords – Cybersecurity Essentials
14	Insider Threat – Blame Game
15	2FA – Factor Fakeout
16	Email – Cybersecurity Essentials
17	BEC – You Never Call
18	Breach Awareness – Readiness and Response

Based on the phishing simulations, identify high-risk users who are most likely to click on phishing links and target them with remedial training. You may also choose to include users who present a high risk for spear phishing/targeted attacks because of their role within the organization. This may include employees in Accounting/Finance, HR, IT and executive staff.

Recommended Training Courses:

- Phishing – Understanding Phishing
- Spear Phishing – A Terminal Mistake
- Email Attachments – Scams Gone Viral

9. Communicate results

A great way to raise awareness and increase the impact of your phishing campaigns is to share the results across the organization. Even though Webroot® Security Awareness Training lets you see who clicked on what, the goal is to capitalize on everyone's engagement by sharing aggregate results — not to call out individuals. People will instantly recognize if they clicked or were "phished". More importantly, seeing the statistics on where the organization stands as a whole sets the expectation for further engagement.

After the baseline phishing simulation, send out an email to all employees with the results and the reasoning for the campaign. This is also an opportunity to introduce the training program you will run over the coming weeks and months. Consider including our phishing infographics as part of your communications to employees or hang them up as posters to help keep security top of mind.

To communicate training progress and more detailed phishing simulation results, try using one of the built-in campaign summary reports and customizing the content to meet your organization's needs.

10. Calculate the return on security investment (ROSI)

After 12 months of training, end users are 50% less likely to fall for a phishing attempt based on our latest data. Use the ROSI calculation for cost benefit analysis during your first annual review to demonstrate the real savings to management teams or, if you are an MSP, to clients using Security Awareness Training.

ALE = Average Loss Expectancy = Cost per incident times the # of incidents

Mitigation Ratio = Efficacy of solution at stopping attacks as a percentage

Conclusion

We hope these steps show that the mechanics of security awareness training are straightforward, and that our recommendations help you address barriers you may face when introducing cybersecurity, compliance and phishing education to your organization.

The keys to a successful program are that it is continuous, relevant and emotionally engaging — helping employees see how training benefits them in both their work and personal lives.

Webroot remains committed in our mission to help organizations deliver successful security awareness training by simplifying the operation of these programs and delivering new, high-quality training content every month.

[1] Verizon. "2020 Data Breach Investigations Report." (May 2020)

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.