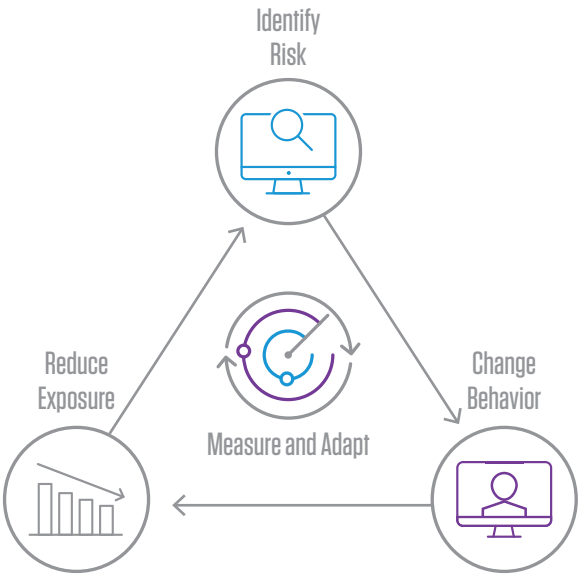


Working Remotely in an Emergency

☑ Campaign Plan and Materials

Gather everything you need to run a successful campaign — done!

☐ Program Continuity Advice

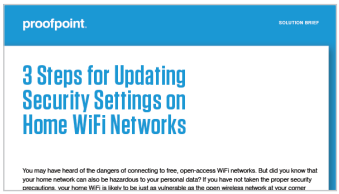
Learn why awareness training is critical during an emergency.

☐ Sample Communications

Introduce security content to end users and stakeholders.

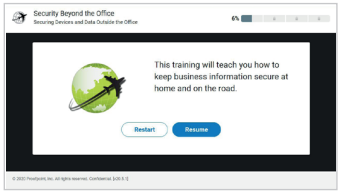
☐ Awareness Flyers

Raise awareness of security basics for working remotely



☐ How-To Article

Guide users on securing their Wi-Fi and home networks.

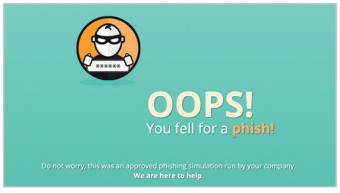


☐ Training Module

Teach users to avoid common security mistakes while working remotely.

☐ Simulated Phish

Assess users with a timely phishing template.



☐ Teachable Moment

Help users who fall for a simulated phish

Consider These Additional Actions ...

Reduce Exposure

Implement our PhishAlarm® and CLEAR to automate email reporting and remediation.

Working Remotely in an Emergency

Tips and guidance for informing users of best practices and raising awareness

Your organization may suddenly need a large population of employees to work remotely, due to a local, regional, national, or global emergency. When situations like these arise, straightforward cybersecurity guidance is critical. Employees need to understand that working remotely requires additional security measures. They also need to be aware that attackers will try to exploit the feelings of fear, curiosity, and uncertainty that are natural during a crisis.

How to Use This Campaign

This document contains suggested communications and resources to help you familiarize your end users with best practices for working remotely and keeping security top of mind during an emergency. Since emergency scenarios vary widely, we encourage you to choose the resources and timeline that make the most sense for your situation. We also suggest that you modify our suggested communications to reflect your company culture, organizational structure, and budget.

Program Continuity Advice

When infosec and IT resources are constrained due to prolonged emergency, curtailing security awareness training initiatives can offer a quick way to free up time and staff members for business-critical continuity exercises. But in times of crisis, cybersecurity best practices can be more critical than ever.

To learn why (and how) to continue security awareness training during such an emergency, we encourage you to review the following document from the downloaded zip file. Share the document with stakeholders and decision-makers who are uncertain whether to continue or pause a program during a prolonged emergency.

- 5 Considerations for Security Awareness Training During Emergency Situations

Sample Communications

As a first step, use our sample email copy to alert your end users, management, and other stakeholders about the goals and purpose of this campaign. These communications can help avoid confusion and drive awareness and engagement.

Email for End Users

Copy and paste the following text into an email. Modify as appropriate before sending to end users.

SUBJECT: Staying cybersecure while working remotely

As we all know, working remotely during an emergency can have unforeseen challenges. It can also introduce cybersecurity risks that might be new to you. In addition, scammers often take advantage of an emergency or crisis. That means we are likely to see scams that try to use this situation to trick us into making decisions that can harm us on a personal or professional level.

To help you stay safe during this emergency, we'll be sending you a variety of cybersecurity resources over the next [time frame]*. Many of the tips and advice we share with you can be passed along to friends and family members, who may also benefit from greater attention to cybersecurity behaviors during this time.*

In the meantime, please be particularly vigilant about the email you receive. It's especially important to be on the lookout for fraudulent emails about [current emergency]*. These phishing emails generally try to use fear, curiosity, and uncertainty to trick recipients into clicking malicious links, downloading dangerous attachments, and visiting lookalike websites that steal personal information.*

Email for Management and Stakeholders

The following text can be used to communicate with stakeholders in technical, managerial, and executive roles. Modify as appropriate before distributing.

SUBJECT: Defending remote workers against cyber attacks

Scammers often take advantage of emergencies and crises to attack individuals and organizations. For example, they may draw upon [current emergency] *to create convincing phishing emails, designed to trick end users into interacting with malicious links, attachments, and websites.*

Keeping security top of mind is especially important when individuals are working remotely. They need additional guidance to help them avoid risky behaviors and identify potential threats. To protect our organization, we're rolling out an awareness campaign beginning [date]*. The materials we will share will remind employees about best practices for working remotely during an emergency, and provide tips and advice for remaining secure over the coming weeks.*

Online Meetings

In addition to communicating via email, consider briefly introducing your awareness campaign during an online meeting. Since many organizations increase "town hall"-type meetings during emergencies, it's worth asking if you can get 15 minutes added to the agenda. It's an opportunity to make sure people understand why you are running the campaign, touch on how much more prevalent threats are during emergencies, and reinforce the need to stay vigilant.

Security Awareness Training Materials

Awareness Posters

Circulate posters to remind end users about best practices when working remotely and to reinforce positive behaviors. Share them via email or enterprise social channels, or add these materials to your intranet.

Consider rotating poster designs periodically to help keep end users vigilant. We've also provided sample text you can use to introduce this content.

If you are a Proofpoint Security Awareness Training customer, our Security Awareness Materials offer a wealth of flyers and posters in a variety of topics and creative styles to fit your specific needs. You can further customize awareness materials by downloading original art files, which allows you to modify the text as needed and/or add your organization's logo and other branding. If you are not a customer, we have provided a few awareness posters with this download, which specifically address the challenges of working remotely.

- Security Essentials Work Remotely
- Working Remotely Safeguards

Consider using the following text to introduce these posters via email. Modify as appropriate before sending.

SUBJECT: Security tips for working remotely

As discussed, we'll be sending you a variety of cybersecurity resources during this emergency. The attached poster has a quick list of best practices for staying safe while working remotely.

We hope you'll find these tips helpful — and consider sharing this advice with friends and family members. As always, please be particularly vigilant about the email you receive.

You may also want to remind users about the need to always protect data privacy, lock their devices and secure important files, even if they are working from home. We have provided the following resources for your use

- Keep Private Data Private Awareness
- Lock Up When You Leave Awareness

Consider using the following text to introduce these materials via email or other channels. Modify as appropriate before sending.

SUBJECT: Lock Before You Walk – Even at Home

If you're working from home during this emergency, you might feel comfortable leaving important work papers out in the open, or walking away from your work computer without locking the screen. But even though you're not at work, these are still security risks.

For example, someone in your house could decide to use your unlocked computer to check their personal email. They could accidentally click on a malicious website or download an infected attachment, putting you and our organization at risk.

The attached flyer is a quick reminder to maintain good security habits when working remotely — even at home.

How-To Article

When many people will be working from home, it's a good opportunity to remind people that their home Wi-Fi networks must also be secure to protect themselves and your organization. The following "how-to" article is attached.:

- 3 Steps for Updating Security Settings on Home Wi-Fi Networks – Awareness Article

Consider using the following text to introduce this article via email or other channels. Modify as appropriate before sending.

SUBJECT: 3 steps to improve your Wi-Fi security

When working remotely, the security of your home Wi-Fi network is very important. A poorly secured network is vulnerable to attackers and could put you and our organization at risk.

The attached article walks you through three steps to secure your Wi-Fi network — why not take a few minutes right now to make sure you're protected?

Training Modules

Our Security Beyond the Office training is particularly relevant and available for free through July 1. Simply share this link (https://beyondtheoffice.wombatsecurity.com) with your end users. In this module, employees will learn best practices for keeping your data, network, and equipment safe when working outside the office. Topics include safe use of Wi-Fi networks, the dangers of public computers, and practical physical security measures.

Note: *You may notice that the Security Beyond the Office training module is hosted on wombatsecurity.com. Wombat Security Technologies was acquired in 2018 and is now Proofpoint Security Awareness Training.*

Simulated Phishing Template and Teachable Moment

Since attackers often use emergencies and crises to create convincing phishing emails, we believe it's very important to assess your users' vulnerability to such threats. If you are a Proofpoint Security Awareness Training customer, our ThreatSim® Phishing Simulations tool have timely templates powered by Proofpoint Threat Intelligence and will allow you to create a phishing test and choose a follow-up Teachable Moment. that align well with your current emergency.

A Note on Additional Content

Proofpoint Security Awareness Training customers with a Security Awareness Materials license, can find more campaigns like this one, and a variety of other posters, flyers, infographics and videos to fit your organization's culture.

LEARN MORE

For more information, visit **proofpoint.com**.