livingsecurity

Supplemental Training Plan (STP) - “Simon Said”

“Simon Said” is a fun, post-episode email series which follows the eccentric protagonist, Simon, through the Cyber Escape storyline to explore plot-twists, reinforce security concepts and help shape culture.

Please utilize the email templates below in order to engage your team to get excited and compete in the Living Security Platform training series! These were written and timed for the delayed release schedule but can be used during the continuous games to reinforce training concepts and continue to drive participation back to the platform.

Directions

- Insert your personalized content into highlighted sections below
- Send these emails according to the schedule outlined below
- Contact Living Security if you have questions or need additional tools to get your team excited!

Sending Schedule

Week	Send Time	Content
1	Start of week 1, drive people to platform first-time	*Page 2*
2	Start of week 2, drive people back to platform after playing episode 1	*Page 3*
3	Start of week 3, drive people back to platform after playing episodes 1 & 2	*Page 4*
4	Start of week 4, after playing episodes 1, 2 & 3	*Page 5*
5	After playing all episodes, 1-4	*Page 6*

Subject Line: Living Security - Ready to Play!

[Your Greeting Here],

[IT/cybersecurity Intro]!

We'd like to formally welcome you to the Living Security Platform! It is a fun, intuitive platform that brings storylines and security concepts to life. This is security awareness training reimagined… jam-packed full of live-action videos, digital escape experiences and
healthy competition for a top-spot on the company leaderboard!

Here's the link to play if you haven't signed up already:

clientname.livingsecurity.com

These episodes are not just academic but based on real policy abuses observed in our workplaces. Please contact us if you have any questions or want to discover new ways to
secure your digital life.

Your security team,

[Your Sign-Off Here]

Subject Line: What will happen to Simon next?

[Your Greeting Here],

[IT/cybersecurity Intro]!

We'd like to welcome you back to the Living Security platform! By now you should have played episode one and seen that this is a fun way to learn security and help shape our culture to be strong and resilient against cyber threats. This week you'll play episode two and learn some more valuable information about password myths and tips for reclaiming your privacy.

To progress you along in the storyline, we're forwarding a message from the Platform's liaison, Avery, with more instructions...

> *$ ./Hey Remote Team!*
>
> *It's Avery, your tech team liaison. By now you've met our person of interest, Simon, an eccentric, mad-scientist who's used his passion for science to bring a robot to life in his own image. He's stuck in prison trying to explain his way out of a sticky situation. Anyway, you've helped us find a likely location and we're hot on the robot's trail now, but will need your help to access the building. Log back into clientname.livingsecurity.com to investigate… Good luck! Talk soon...*

Link here to play: clientname.livingsecurity.com

Last episode focused on over-sharing while on social media. By geo-tagging your travels and checking in at new locations, you are essentially telling the public where you are AND where you aren't. This information is dangerous in the hands of a criminal - especially when enough data is posted to identify patterns in your daily or weekly routines.

By keeping personal details personal and deleting old accounts, you can reduce your digital footprint. By toggling off location sharing on your applications and devices, you can reclaim your privacy now.

Contact us if you have any questions or want to discover new ways to secure your digital life. Have fun this week learning more!

Your security team,

[Your Sign-Off Here]

Subject Line: Solve Your Next Puzzle

[Your Greeting Here],

[IT/cybersecurity Intro]!

It's that time again! By now you should have played episodes one and two and seen the protagonist, Simon, tumble headlong into a series of unfortunate events. This week you should start by completing Episode 3 to learn about the ways in which internet of things (IoT) devices are vulnerable to cyber attack.

$ ./Remote Team!

It's Avery, again. Awesome job on the pincode puzzle. As MJ said, "random is more predictable
than you'd think." When people set pincodes or passwords, they're often thinking about the
things they can remember, not the strongest string of characters. If you haven't already, jump
back on the platform and see if you can help the team on the ground solve the next puzzle…
Your help is invaluable. Anyway, got to go! Over and out...

Link here to play:clientname.livingsecurity.com

These episodes are not just academic but based on real policy abuses observed in our workplaces. For example, the episode last week focused on password creation. Of course,
it's necessary to comply with company policy [insert policy here]. But new security measures promise to improve your convenience and privacy, too. Consider the following tips:

- Use passphrases
- Enable multi-factor authentication
- Use a password manager

Every year, weak passwords and poor cyber hygiene habits cost organizations billions of dollars annually. Your diligence will fix new problems before they crop up and old problems
at their root. Carelessness costs time, money and jobs. Caring is free :)

Contact us if you have any questions or want to discover new ways to secure your digital life. Good luck this week!

Your security team,

[Your Sign-Off Here]

Subject Line: Can You Find the Robot?

[Your Greeting Here],

[IT/cybersecurity Intro]!

We'd like to welcome you back to the fourth and final week of the Living Security Platform Training! This is it! The grand finale… the coup de grace… and it just might have you on the edge of your seat.

To finish out the storyline, we're forwarding along a final message from the Platform's liaison, Avery, with time-sensitive instructions...

> *$ ./Remote Team!*
>
> *It's me! Hey, we're hot on the trail of this rogue bot… I can feel it. Your help identifying those internet of things (IoT) devices in the shared workspace to force the bot to shut down was awesome. Let's see if they can wrap this case up and report back to HQ. I think we're right on the precipice of a breakthrough. My spidey senses are tingling, though. This one feels like we're not going down without a fight. Be bold! Don't let the robot go quietly into that goodnight! <static> End Transmission…...*

Link here to play: xyz-ce.livingsecurity.com

That third episode got us even closer to the action and focused us in on internet of things (IoT) devices and their inherent vulnerabilities. It is not just semantics. Just last year, a large collection of internet devices with default credentials -- passwords set by the manufacturer and never changed -- were turned against their owners and used to attack Twitter, Facebook and others in a distributed-denial of service attack. (For more details, just ask us!)

Instead of buying a new smart device and getting a free vulnerability, try these things to secure them:

- Change default passwords
- Install software updates
- Backup your devices

You're doing well and nearly there! Keep up the good work. And contact us if you have any questions or want to discover new ways to secure your digital life.

Your security team,

--

[Your Sign-Off Here]

Subject Line: Trust Your Training!

[Your Greeting Here],

[IT/cybersecurity Intro]!

Success! Amazing job being the remote team in this cyber adventure of security and intrigue.

In that thrilling finale, we were thrust into a world of chaos and technology, much like the one we live in today. Your help identifying social media profiles, weak passwords, vulnerable IoT devices and phishing emails has prepared you for this brave new world. So don't trust what Simon says… trust your training! And when in doubt, we'd love to talk more or answer any questions.

Here's three tips to digital freedom in the workplace and in your private life:

- Feel no curiosity
- Suspect before you Inspect
- Tune your inbox (unsubscribe from meaningless mail, mark spam as spam and organize the rest into folders)

Thank you for playing! We hope you enjoyed this adventure just as much as we enjoyed providing it. As always, please contact us if you have any further questions or want to discover new ways to secure your digital life. And if you have any feedback on the Living Security Platform or thoughts on how we can improve security training for you, please let us know. Be the next strong link in the chain!

Your security team,

--

[Your Sign-Off Here]

Thank you!

The Living Security team greatly appreciates all of your time and dedication to inspiring your team to participate in the Living Security Platform. We would appreciate any feedback you or

your team have on the platform and on the training affects your organization sees over the long term.

If you are interested in other gamified security training tools, please check out our website or shoot us a message!