Steps to setting up your 'Are you 21st Century Ready?' Quiz

1. Create an account on the free interactive quiz platform: http://www.riddle.com/.
2. Open the following link: http://www.riddle.com/a/8186, where we have set up the quiz for you.
3. Click the word "Copy" located on the upper right corner of the webpage above to duplicate the quiz onto your own dashboard.
4. Return to your Riddle dashboard and you should see the copied test there: *"[Copy] Are you 21st century ready?"*
5. You now have your own version of the 'Are you 21st Century Ready?' Quiz and can share the link with your company's employees to complete.
6. Share this survey with employees by either sending out an email with the link and/or embedding the link on your company's internal communications channels, such as the Intranet platform.
7. Review employee scores by accessing your Riddle dashboard and clicking on the bottom right link that looks like a graph.

   A series of metrics will be available for your review, but the following are the ones which are recommended for you to take note of:

   a. Percentage of users that received each personality profile

      i. If most employees receive the *Almost at the finish line* score card, your corporate cybersecurity agenda is on track and executing the rest of the Kit will only help to boost it.

ii. If most employees receive the *You're getting there* score card, you need to work a little bit more on your corporate cybersecurity agenda. Executing the rest of the Kit will help to make your employees more prepared to guard against cybersecurity threats.

iii. If most employees receive the *Still at the starting line* score card you need to step up on the corporate cybersecurity agenda. Consider also utilising the Employee Cyber-readiness Kit from Level 1.

b. <u>The number of people that finished the quiz</u>

You can compare this number to the actual number of employees expected to complete this quiz. If it falls short, consider sending out a reminder e-mail to employees to complete this quiz a week after the first e-mail was sent out.

c. <u>The number of people that shared the quiz</u>

This helps you to track if there might be people outside of the company who are completing the quiz and show just how popular this quiz is with employees, as they took the extra effort to share it.

"Are you 21st Century Ready?" Quiz Questions

Introduction

Welcome to the "Are you 21st century ready?" Quiz! At the end of this quiz, you'll find out if you are equipped enough to survive the 21st century and protect against the many cyber threats we face out there. These 11 questions should take you just 3-5 minutes to complete.

1. **When it comes to maintaining your password security, how would you describe yourself?**
    a. Creative, I use different variations of one master password for my accounts
    b. Forgetful, I use the same password for all my accounts
    c. Masterful, I have different passwords for each account

2. **If my company didn't force me to change my password every few months, I would…**
    a. Change it regularly for my own security
    b. Change it only because I've forgotten what it was…
    c. Keep the same password that I've had from day one

3. **While visiting a website, a message pops up: "You just won $100,000! Click here to claim your prize". What would you do?**
    a. Claim my prize!
    b. Exit the pop-up immediately
    c. Check out if the offer is legitimate by testing the link

4. **When was the last time you changed your password for your personal email address?**
    a. Within the last few months
    b. Within the last year
    c. It's been so long I don't even remember

5. **What about your work email password?**
    a. Within the last year
    b. Within the last few months
    c. So glad my IT department doesn't make me change it, because I never do

6. **How much personal information do you share on your social media accounts?**
    a. Everything there is to know about me, it's my digital diary!
    b. Stuff that everyone who follows me should know

c. Only the basics (hobbies, favourite movies, food and books, line of work)

7. **How do you keep track of your passwords?**
    a. I scribble them on a piece of paper or in a notebook
    b. I store them in my password mobile app
    c. I memorise them!

8. **When I'm prompted to upgrade my software, I tend to:**
    a. Comply and click 'install'
    b. Procrastinate for a while before actually doing it Avoid it until I'm forced to do so

9. **You receive an e-mail from your bank about a problem with your account. The e-mail provides instructions and a link for you to log in and fix the problem. What would you do?**
    a. Check it out and close the window if it looks suspicious
    b. Contact the sender directly to verify that the message is from them
    c. Close the e-mail and trash it

10. **What do you do when you have to leave your computer unattended for a while?**
    a. Shut down, log off, or lock it
    b. Turn off the monitor or lower my laptop screen down
    c. Nothing, I'm only going to be gone for a few minutes

11. **You're waiting for your order at Starbucks and decide to connect to their free Wi-Fi. While connecting to Gmail, the page redirects you to http://www.googlemail.michael.net. What do you do?**
    a. Disconnect immediately
    b. Don't even notice the URL is different from the usual one
    c. Ask the person next to you if his Gmail also redirects in a similar fashion

Quiz Scorecard

ALMOST AT THE FINISH LINE

You know right from wrong, and tend to practise good cybersecurity habits whether you're at home, holiday, or at the office. It's important to keep in mind that cybercrime is on the rise and will continue to evolve, so there will always be new security practices to enact. Don't get complacent, keep at it!

- Three tips to get you to the finish line:

    1. **Read privacy policies:** Yes, they can be complex, but they can help you keep yourself and your loved ones safe. They tell you how the site maintains accuracy, access, security, and control of the personal information it collects; how it uses the information, and whether it provides information to third parties.

    2. **Share your wisdom**: Not everyone knows the basics, so when you can, pass on your knowledge to a few colleagues. Your entire company's security is only as strong as its weakest link.

    3. **Back it up**: It's not *if* you lose your data, but *when*. It's always better to be safe than sorry!

YOU'RE GETTING THERE

You have good instincts, but that's not enough to stay safe in the 21st century. Brush up on your cybersecurity knowledge! As long as we use technology, we are vulnerable to someone or something accessing or corrupting our information. Let's be sure to develop habits to make it more difficult for them to do so. Don't fall prey to an attack!

- Three tips to get you there:

    1. **Always check the source**: Phishing e-mails might look legitimate or send you to websites that appear official, so always check for the sender of the email and the URL of the links that have been sent.

    2. **Watch where you surf**: If you have to, only enter personal and financial information on websites that have the prefix "https," which signals deeper

encryption.

3. **Update your software:** Those app updates you've been ignoring could be security fixes that might plug loopholes in your system.

STILL AT THE STARTING LINE

Thinking about cybersecurity may feel overwhelming and mind-boggling, but it's a lot easier than you think! If you start with simple steps and practise them daily, you can avoid potential catastrophic attacks on personal information, work systems and even the nation's critical infrastructure. Any network is only as strong as its weakest link. Don't be an easy target for cyber criminals!

- Three tips to start you off:

1. **Make passwords long and strong:** All passwords should be at least 10 characters and include lower and upper case letters, numbers, and symbols. Can't remember them? There's an app for that.
2. **Be wise about Wi-Fi:** Think twice before connecting to a public wireless network. And if you do, use a VPN and switch on your antivirus and firewall.
3. **Run anti-virus software:** Anti-virus software provides protection by scanning for and removing malicious files on your computer.