

แบบทดสอบก่อนเรียน
เรื่อง การใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย

คำชี้แจง ให้นักเรียนเลือกคำตอบที่ถูกต้องที่สุด 1 ตัวเลือก

1. รหัสผ่านที่ปลอดภัยควรมีลักษณะอย่างไร?
 - ก. ตัวเลขง่าย ๆ เช่น 1234
 - ข. มีตัวอักษรพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และสัญลักษณ์
 - ค. ใช้ชื่อหรือวันเกิด
 - ง. ใช้คำว่า “password”
2. เว็บไซต์ที่ปลอดภัยสำหรับธุรกรรมออนไลน์มักจะมีอะไรใน URL?
 - ก. http://
 - ข. https:// และมีสัญลักษณ์กุญแจ
 - ค. ftp://
 - ง. www.
3. ข่าวลวงคืออะไร?
 - ก. ข่าวที่ถูกต้องและตรวจสอบได้
 - ข. ข่าวที่บิดเบือนหรือสร้างขึ้นเพื่อหลอกกลาง
 - ค. ข่าวที่เผยแพร่ในสื่อหลักเท่านั้น
 - ง. ข่าวที่มาจากสำนักข่าวที่มีชื่อเสียง
4. ข้อใดช่วยป้องกันไวรัสคอมพิวเตอร์ได้ดีที่สุด?
 - ก. ไม่ใช้คอมพิวเตอร์เลย
 - ข. ติดตั้งและอัปเดตโปรแกรมป้องกันไวรัสเสมอ
 - ค. เปิดลิงก์ในอีเมลที่ไม่รู้จัก
 - ง. ดาวน์โหลดโปรแกรมจากเว็บไซต์ไม่รู้จัก
5. ฟิชซิง (Phishing) หมายถึงอะไร?
 - ก. การส่งอีเมลหรือข้อความปลอมเพื่อขโมยข้อมูลส่วนตัว
 - ข. การอัปเดตระบบปฏิบัติการ
 - ค. การติดตั้งแอปพลิเคชัน
 - ง. การสร้างเว็บไซต์ใหม่
6. การใช้ Wi-Fi สาธารณะควรระวังอะไร?
 - ก. ทำธุรกรรมออนไลน์ทันที
 - ข. ใช้ VPN เพื่อปกป้องข้อมูล
 - ค. ใช้รหัสผ่านเดียวกันทุกเว็บไซต์
 - ง. แชร์ข้อมูลส่วนตัวกับเพื่อน
7. รหัสผ่านควรมีความยาวขั้นต่ำกี่ตัวอักษร?
 - ก. 4 ตัว
 - ข. 6 ตัว
 - ค. 8 ตัว
 - ง. 12 ตัวขึ้นไป
8. หากได้รับอีเมลขอข้อมูลส่วนตัว ควรทำอย่างไร?
 - ก. ส่งข้อมูลทันที
 - ข. ลบและไม่ตอบกลับ
 - ค. แชร์ให้เพื่อนดู
 - ง. คลิกลิงก์ในอีเมล
9. ข่าวลวงมักมีลักษณะอย่างไร?
 - ก. มีแหล่งข่าวชัดเจน
 - ข. ใช้คำพูดเกินจริงหรือสร้างความตื่นตระหนก
 - ค. มีข้อมูลทางวิชาการรองรับ
 - ง. มีการอ้างอิงข้อมูลอย่างถูกต้อง
10. การรู้เท่าทันสื่อหมายถึงอะไร?
 - ก. เชื่อทุกข่าวที่ได้รับ
 - ข. ตรวจสอบและประเมินข้อมูลก่อนเชื่อหรือแชร์
 - ค. ไม่ใช้สื่อออนไลน์เลย
 - ง. แชร์ข่าวทันที
11. ข้อใดช่วยให้ธุรกรรมออนไลน์ปลอดภัย?
 - ก. ใช้รหัสผ่านเดียวกันทุกเว็บไซต์
 - ข. ตรวจสอบความถูกต้องของเว็บไซต์ก่อนกรอกข้อมูล
 - ค. คลิกลิงก์ในอีเมลไม่รู้จัก
 - ง. แชร์ข้อมูลส่วนตัวในโซเชียลมีเดีย
12. ข้อใดคือวิธีที่ช่วยป้องกันการถูกโจมตีทางไซเบอร์?
 - ก. ใช้รหัสผ่านง่ายๆ เพื่อจำได้ง่าย
 - ข. ไม่อัปเดตซอฟต์แวร์
 - ค. ใช้โปรแกรมป้องกันไวรัสและอัปเดตอย่างสม่ำเสมอ
 - ง. คลิกลิงก์ทุกลิงก์ที่ได้รับในอีเมล

13. การใช้รหัสผ่านเดียวกันในทุกเว็บไซต์ปลอดภัยหรือไม่?
- ก. ปลอดภัย
 - ข. ไม่ปลอดภัย
 - ค. ขึ้นอยู่กับเว็บไซต์
 - ง. ไม่มีความสำคัญ
14. การแชร์ข่าวสารโดยไม่ตรวจสอบความถูกต้องอาจทำให้เกิดอะไร?
- ก. สร้างความเข้าใจผิดในสังคม
 - ข. ช่วยเผยแพร่ข้อมูลที่ถูกต้อง
 - ค. ทำให้ข่าวน่าเชื่อถือ
 - ง. ไม่มีผลใด ๆ
15. ข้อใดไม่ใช่พฤติกรรมที่ปลอดภัยในการใช้งานอินเทอร์เน็ต?
- ก. อัปเดตซอฟต์แวร์และระบบปฏิบัติการอย่างสม่ำเสมอ
 - ข. เปิดไฟล์แนบจากอีเมลที่ไม่รู้จัก
 - ค. ใช้รหัสผ่านที่แข็งแรง
 - ง. ใช้โปรแกรมป้องกันไวรัส
16. การคลิกลิงก์ในอีเมลที่ไม่รู้จักอาจทำให้เกิดอะไร?
- ก. เครื่องติดไวรัสหรือมัลแวร์
 - ข. เครื่องทำงานเร็วขึ้น
 - ค. ไม่มีผล
 - ง. ได้รับข้อมูลเพิ่ม
17. การตั้งรหัสผ่านที่ดีควรประกอบด้วยอะไรบ้าง?
- ก. ตัวอักษรพิมพ์ใหญ่และเล็ก
 - ข. ตัวเลข
 - ค. สัญลักษณ์พิเศษ
 - ง. ทั้งหมดที่กล่าวมา
18. ถ้าคุณสงสัยว่าเว็บไซต์ไม่ปลอดภัย ควรทำอย่างไร?
- ก. กรอกข้อมูลตามคำขอ
 - ข. ออกจากเว็บไซต์ทันที
 - ค. แชร์เว็บไซต์นั้นให้เพื่อน
 - ง. ใช้เว็บไซต์ต่อไป
19. การรู้เท่าทันสื่อช่วยให้คุณทำอะไรได้ดีขึ้น?
- ก. เชื่อข่าวทุกข่าว
 - ข. แยกแยะข่าวลวงและข้อมูลที่ถูกต้อง
 - ค. แชร์ข้อมูลทุกอย่างทันที
 - ง. หลีกเลี่ยงการใช้สื่อออนไลน์
20. อะไรคือสิ่งสำคัญที่สุดในการป้องกันธุรกรรมออนไลน์?
- ก. รหัสผ่านที่ปลอดภัยและตรวจสอบเว็บไซต์ก่อนกรอกข้อมูล
 - ข. แชร์ข้อมูลกับเพื่อน
 - ค. ใช้ Wi-Fi สาธารณะในการทำธุรกรรม
 - ง. บันทึกรหัสผ่านลงในไฟล์ที่เปิดเผยมง่าย