Secure My Life: Resources

There are 7 items in the Resources section.

“I Have Ransomware” Article

Article from CyberSafety Daily with details on what you may see on your screen if your device has ransomware.

- Lock icons - show files are encrypted (locked)
- “Pay with Bitcoin” options - show preferred currency in ransomware schemes, which is harder to trace
- Countdown timer - adds a sense of urgency and encourages you to act without considering options
- Threat to “double the payment” - another way to make you panic and act quickly
- “Contact Us” button - may be bait to give up more personal information or make things worse and should be avoided
- Unknown links - can lead to worse things, so never copy, paste, or click these

Secure My Life: Resources

Web Article

Article from CyberSafety Daily explaining what Bitcoin and Botnets mean

Bitcoin

- Most popular and widely used form of cryptocurrency
- Not insured by banks or the government
- Not tracked when bought, sold, or converted from your accounts
- Anonymous and untraceable online
- Can be purchased using money or mined online with computers and/or botnets

Botnets

- Networks of hijacked computers
- Can be used to spread malware, mine for cryptocurrency, and/or to carry out cyber attacks
- Hacked into by criminals, who then take control of the computer remotely for their own use
- Can eventually slow down or crash devices hosted on over time

Secure My Life: Resources

Category List

Two notebook pages with hand-written classification of files as either personal or work

Personal

- Family photos
- Social media
- Games (entertainment)
- eBooks
- Personal projects
- Online shopping

Work

- Client information
- Professional projects
- Company email
- Business contacts
- Billing statements and/or finances
- Client contracts

Security Tips Checklist

Checklist for the Top 10 Cybersecurity Tips

Do:

- Change your passwords regularly
- Think before you click on pop-ups like online advertisements
- Avoid downloading unknown videos or apps, as free doesn't always mean safe
- Keep devices and software up to date
- Enable multi-factor authentication everywhere you can
- Verify contact and friend requests online

Don't:

- Add strangers who send friend requests
- Respond to suspicious emails, texts, or calls
- Reveal personal information online, like your birthday or address
- Click on unknown or suspicious links
- Share your passwords with anyone, even friends and family

Secure My Life: Resources

How to Catch a Fish

9 safety tips to avoid phishing attacks on social media

1. Look out for misinformation
2. Beware fake advertisements
3. Don’t get hooked by social engineering bait
4. If the person who sent a friend request has few or no mutual friends, decline
5. Recent join dates can mean a fake account
6. Look for real photos of people, not stock images or silhouettes
7. Inspect unknown links before you bite
8. Loose lips sink ships – watch out for misspelling and poor grammar
9. Avoid automated responses

Secure My Life: Resources

Sticky Note

Handwritten sticky note with thoughts

- What is ransomware?
- Options?
- How to stay safe?

Testimonials

Online testimonials from victims of ransomware

Sandy P.:

“My company had a run-in with ransomware. It cost us millions of dollars to pay the ransom, and a few people even got laid off. Thank goodness the criminals gave us back access after paying. You never know what clicking a bad link can do.”

Karen M.:

“BEWARE!!! I paid off ransomware before, and I STILL didn’t get my stuff back! THEY ARE CRIMINALS. Nothing but a bunch of LIARS.”

Secure My Life: Resources

Testimonials, continued

Roger W.:

"I got ransomware on my laptop. I'm only 14, so I didn't have the money to pay what they wanted, and I was too embarrassed to tell my parents. I lost all my music, photos, and pretty much my whole life. It really stinks. Now I always back up my stuff and save copies on a hard drive - just in case."

Fernando G.:

"Remember guys: you don't have to pay. My wife and I had to make the tough decision to lose some really important files a year ago when we got ransomware... but we didn't want to give these people any of our money."

Secure My Life: Exercises

livingsecurity

There are 8 exercises throughout the game:

1. In exercise 1, you are identifying six clickable areas in an image that may be tied to ransomware. Refer to the “I Have Ransomware” Article in the Resources section to complete the exercise.

2. In exercise 2, you need to choose three questions to identify the area Johan has the worst security in. Use the Security Tips Checklist from the Resources section to help.

3. In exercise 3, you must review Johan’s social media account and click on the red flags that could have alerted him to ransomware. Check out “How to Catch a Fish” in the Resources section to know what to look out for.

4. In exercise 4, you are talking to Peter, a ransomware expert, on the phone. Look at Saanvi’s Sticky Note in the Resources section to guide the conversation.

5. In exercise 5, you need to map out the options for Peter, to help him decide whether or not to pay the ransom. Examine the Testimonials in the Resources section to finish this exercise.

Secure My Life: Exercises

livingsecurity

Exercises, continued

6. In exercise 6, you are finding missing words in sentences about digital currency. Check out the Web Article in the Resources section. Then, drag the right words into the correct slots to complete the exercise.

7. In exercise 7, you are helping Johan decide if files belong on a work device or a personal device. Refer to the Category List from the Resources section to determine the correct classification for each item, then drag it into place in the puzzle.

8. In exercise 8, you are answering a series of open-ended questions to summarize what you learned in the game.