**Hints**

Open Source Intelligence:

Find the underlined words and their corresponding number, write these down on your scrap paper. You will get more word, number pairs in other puzzles, the number will order the words to form the question that you will need to solve.

Phishing Hint:

Remember, you are looking for the LEGITIMATE email, not the fraudulent ones, recall that creating a sense of urgency is a common tactic in Phishing scams.

Botnet assembly:

When sorting alphabetically make sure to note the word given in the even numbered positions. Then sort by the third number in the device ip address, this will result in word number pairs used to form a question that you will answer to proceed

Puzzle Group 1 Hint (how to assemble the security question)

Use the number word pairs you have obtained and order the words in the order of their corresponding number.

Puzzle Box Hint:

Flip it over. Try hitting it. (Seriously)

Bruteforce Hint:

Try all the combinations of the given digits. For example, if the given digits were one, two, and three, you would try 123, 321, 213 etc.

QR Code Hint (Puzzle Group 2)

Make sure the QR code is flat, that the sections are in the right place, and that there is no overlap or gaps when scanning the code

Fold Puzzle Hint (how to do it)

Fold the paper so that the labeled semi circles that share an order are touching. Fold from least to greatest.

Decryption Hint:

Look through the previous materials carefully, you will find a decryption key. (Tell them where it is (folder) if they do not find it after a minute or two)

Password Hash Hint:

Enter the hash into the hash cracker tool. It will in turn give you the password of the perpetrator’s account.

Vocab Hints

For all vocab hints, tell them to consult the vocab papers.

Botnets: Parties use them to perform coordinated mass attacks to overwhelm systems.

Brute force: An attacker using this approach systematically checks all possible passwords and passphrases until the correct one is found.

Open source intelligence: personal data derived from information that is available to the public.

Phishing: An attacker using this approach would be posing as a trusted entity, and use **social engineering** in order to manipulate users into performing self-harming actions.

Ransomware: It often **encrypts** the software, and will return a **decryption key** once the money is paid.

Encryption: the process of converting information or data into a code.

Hashing: putting a password through an algorithm to turn plaintext into an unintelligible series of numbers and letters.