愛知県警察

サイバーポリスゲーム～組織版～の

「クイズ」マス

の内容をご紹介します。

サイバ課長

マホ巡査

クイズカード

正解したら**ボーナス５０PT**

Ｑ１

“OSINT（オシント）”って何の略？

Ｑ１の選択肢

1. Opportunity Signal into Technology

2. Open Science Initiatives Network Teams

3. Open Source Intelligence

答え＆解説

Ｑ１の答え

3

Ｑ１の解説

オシント
OSINT（Open Source Intelligence）とは、合法的に入手できる資料を集め、それらを突き合わせて対象に関する事象を明らかにする調査手法です。

攻撃側も守る側もどちらも用います。SNSは資料入手の際に一番よく用いられるため、写真や投稿内容を見直さずに投稿すると情報漏えいに結びつきやすいのです。

クイズカード

正解したら**ボーナス５０PT**

Q２

この投稿からわかる情報を**５つ**答えて。

答え＆解説

Ｑ２の解答例

●住んでいる地域　（制服やお店の場所など）

●写真を撮った日時　（SNSに投稿した時間）

●写真を撮った場所　（電柱・マンホール・車のナンバー・お店の看板・限定商品など）

●姿（顔）

●通っている学校名（制服・お店の場所など）

●学校帰りにその場所を通ること（投稿内容、カフェの場所、撮影時間・投稿時間など）

●本名や呼び名（投稿者名：MAHOなど）

クイズカード

正解したらボーナス５０PT

Ｑ３

ユーザとして、長期休暇前にやるべき作業はどれ？（答えは一つとは限りません）

Ｑ３の選択肢

1.機器やデータの持ち出しルールを確認する

2.休暇中に使用しない機器の電源はOFFにする

3.メールの添付ファイルはすぐに開いて確認する

4.事前にOSやアプリのアップデートをする

5.メールの宛先が不審な相手の場合は、相手にメールで確認をする

答え＆解説

Ｑ３の答え

１、２、４

Ｑ３の解説

長期休暇中はいつもと情報機器の管理体制が変わりがちです。
その間を狙ってサイバー攻撃の被害に遭うことが多いため
対策が必要になります。
主な対策は

（１）機器やデータの持ち出しルールを確認して守る

（２）長期休暇期間中に使用しない機器の電源を落とす

（３）事前にOSやアプリのアップデートをする

（４）不審な添付ファイルやリンク先にアクセスしない

（５）不審に思ったらメールを開く前に電話や別の手段で
確認する

です。

クイズカード

正解したらボーナス５０PT

Q４

ユーザとして、長期休暇後にやるべき作業はどれ？（答えは一つとは限りません）

Q４の選択肢

1.持ち出した機器や記録媒体のチェックをする

2.機器の電源を入れる前に１分間お祈りをする

3.始業前にOSやアプリのアップデートをする

4.不審な添付ファイルやリンク先にアクセスしない

5.メールの宛先が不審な相手の場合は、相手にメールで確認する。

答え＆解説

Q４の答え

１、３、４

Q４の解説

長期休暇中はいつもと情報機器の管理体制が変わりがちです。
その間を狙ってサイバー攻撃の被害に遭うことが多いため
対策が必要になります。
主な対策は

（１）持ち出した機器や記録媒体のチェックをする

（２）始業前にOSやアプリのアップデートをする

（３）不審な添付ファイルやリンク先にアクセスしない

（４）不審に思ったらメールを開く前に電話や別の手段で
確認する

です。

クイズカード

正解したらボーナス５０PT

Ｑ５

パスワードを設定する際、他人に推測されて勝手に使われないためには、どんなパスワードがいい？（答えは一つとは限りません）

Ｑ５の選択肢

1.自分の名前と誕生日

2.10文字以上

3.忘れないよう、他で使っているパスワードと同じもの

4.アルファベット、記号、数字を組み合わせる

答え＆解説

Ｑ５の答え

２、４

Ｑ５の解説

パスワードの使い回しは危険です。１か所でもその情報が漏れると他のサイトも攻撃されてしまいます。

＜安全なパスワードの作り方（例）＞

（１）パスワードは**１０文字以上**にする

（２）推測されやすい単語、生年月日等は使わない

（３）大文字/小文字/記号を混ぜて使う

（４）よく使うパスワードにチョコっとプラス

いろは銀行 ⇒ IRH 318daiSUKI!318

アルファベットで「IROHA」　　よく使うパスワード

クイズカード

正解したらボーナス５０PT

Q６

地震発生後、「津波に関する情報はこちら
http://www.abc.efg.jp/ 」
とかかれたショートメッセージがスマホに届いた。
どの行動が正解？？（答えは一つとは限りません）

Q６の選択肢

1.すぐにURLをクリックして、情報を確認する

2.自分で自治体や災害情報のニュースのホームページを検索して確認する

3.テレビ、ラジオを見る

答え＆解説

Ｑ６の答え

２、３

Ｑ６の解説

災害等の混乱に乗じて、偽サイトを使い、個人情報やお金をだましとる事案がよく発生します。慌てる時こそ冷静に。

ショートメッセージのURLは押さず、一度ショートメッセージを閉じましょう。

情報を確認する場合は、公式ウェブサイトや、テレビ、ラジオを確認しましょう。

クイズカード

正解したらボーナス５０PT

Ｑ７

SNSで知り合った相手から古着を購入する約束をして入金したのに、古着が届かない。
どうしたらいいかな？（答えは一つとは限りません）

Ｑ７の選択肢

1.近くの警察署に行って相談する

2.１８８に電話をして相談する

3.１１０に電話をして相談する

4.相手の氏名・住所・口座情報などをSNSに晒す

5.＃９１１０に電話をして相談する

答え＆解説

Ｑ７の答え

１、２，５

Ｑ７の解説

SNSやインターネット上では相手の素性がわかりづらく、詐欺被害が多く発生しています。なるべく信頼できる場所で商品を購入するようにするとともに、相談先をしっかりと把握しておきましょう。

近くの警察署もしくは＃９１１０へ電話

消費者ホットライン１８８へ電話

※１１０番は緊急通報のための番号です。身体・生命の危険性が高い場合以外は利用を控えましょう。

SNS上で相手の氏名・住所・口座情報などを許可なく掲載することは不法行為となります。

クイズカード

正解したらボーナス５０PT

Q８

SNSで「お金が欲しい」と投稿したら、
「良い仕事を紹介するよ」「免許証の写真を送って」
とダイレクトメッセージが届いた。
どうしたらいいかな？（答えは一つとは限りません）

Q８の選択肢

1.応募するために免許証の写真を送る

2.近くの警察署に行って相談する

3.とりあえずダイレクトメッセージに返信する

4.ダイレクトメッセージを無視する

答え＆解説

Ｑ８の答え

２、４

Ｑ８の解説

これはいわゆる『闇バイト』へあなたを誘う危険性のあるダイレクトメッセージです。免許証の写真を送った後は、「お前の個人情報を知っているぞ」と脅し、特殊詐欺や強盗などの犯罪行為に加担させようとします。関わってはいけません！

近くの警察署もしくは＃９１１０へ電話

アルバイトなどは信頼できる求人サイトなどを使い、仕事内容をしっかり確認しましょう！