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】

①Opportunity Signal into Technology

②Open Science Initiatives Network Teams

③Open Source Intelligence

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

【Q１の答え】

③

【Q１の解説】

OSINT(オシント)(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をすると情報漏えいに結びつきやすいのです。

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

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。

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

②10 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

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

【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カ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

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

②１８８に電話をして相談する

③１１０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

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

【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。

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！