☆★サイバーセキュリティ小テスト～マホの一日～★☆

1 メール

おはようございます。
私の朝の仕事のルーティーン（日課）は出勤してすぐメールをチェック！

えっと…取引先からの返信メールに「見積書.zip」が添付されています。
開いていくと「コンテンツの有効化」ボタンが表示されます！
有効を押していいんでしょうか？

Q 「有効化ボタン」どうしますか？

- 押す
- メールで取引先に確認する
- 放置する
- 電話で取引先に確認する

2 パスワード

お昼の時間、休憩タイムです！
SNSを見て、リフレッシュします(^^♪
この頃、いろんなサイトやアプリでパスワード求められますね↘
パスワードの入力って大変ですね。

私の職員番号は010200だから…

名前：マホ

Q 次のうち、最もリスクが低いパスワードは？

- Maho010200
- 123456
- uMebosh!58
- 1qaz2wsx

3 脅威や手口

終業時間まであと少しです⤴
帰ったら撮りためたドラマを見るのを楽しみに、あと一息乗り切ります！

回覧が回ってきたけど、なになに？
「［　　？　　］による被害が
大企業・中小企業等を問わず急増!!」
ですって（゜Д゜）

Q パソコンなどのデータを**暗号化して**使えないようにし、**身代金を要求する**ウィルスは？

- トロイの木馬
- ワーム
- ランサムウェア
- スパイウェア

お疲れ様でした

よしっ、仕事終わり！！
今日は頭をたくさん使ったから疲れちゃいました。

答えと解説は裏面にあります！
皆さん、お疲れ様でした(^^

愛知県警察 AICHI POLICE

☆★～答えと解説～★☆

1 メール

答え. **電話で取引先に確認する**

「コンテンツの有効化」を**押す**とマルウェア（不正なプログラム）に感染するおそれがあります。
相手方に確認する際は、受信した**メール**に返信するのではなく、**電話**等で確認するようにしてください。
その際相手方にも注意喚起をお願いします。

放置せず、情報セキュリティ担当や上司に相談して対応してください。

※実際には社内のルールに沿った対応をしてください。

2 パスワード

答え. **uMebosh!58**

実際、SNSも企業のシステムもパスワードを推測されて不正にアクセスされた被害が多発しています。誕生日や名前、従業員番号、数字のみ、キーボードの配列(1qaz2wsx)など、**推測されやすいパスワードは大変危険**です。

- **長く複雑なパスワード**に設定しましょう
  (10桁以上、大文字、小文字、記号を混在させるなど)
- サイトやアプリごと異なるパスワードを設定し、**パスワードの使い回しはしない**ようにしましょう

■■■より安全なパスワードにするためには■■■■

例）**uMebosh!58→uMb4g8nSk?**

単語を自分なりのルールで不規則な文字列にするなど工夫を凝らしてみましょう！ なお例示のパスワードは使用しないでください。

3 脅威や手口

答え. **ランサムウェア**

ランサムウェアとは、感染するとパソコン等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを元に戻す対価として金銭を要求する不正なプログラムのことです。

感染を放置すると被害が拡大するおそれがありますので、「**LANケーブルを抜いて(Wi-FiをOFFにして)情報セキュリティ担当者に連絡する**」など問題が発生した場合のルールを確認しておきましょう。

☆参考★

～組織の一人ひとりが実践する～

あいち情報セキュリティ五箇条

一、まず知ろう　被害事例や　その原因
被害事例や原因を知ることで、
情報セキュリティに対する意識を高めましょう！

二、その情報　あなた個人の　ものじゃない
業務で取り扱う情報は、個人のものではなく、
組織のものであることを意識しましょう。

三、パスワード　英・数・記号で　複雑に
パスワードは、情報を守る大切な鍵です。
英・数・記号で長く複雑に設定しましょう。
また、同じパスワードの使い回しは大変危険
なのでやめましょう。

四、そのメール　開く前に　確認を
攻撃者は、取引先等を装ったメールでウイルス
感染させようとします。メールにあるＵＲＬや
添付ファイルをクリックする前に一度手を止め、
相手方に確認するなどの方法で、よく確認しましょう。

五、その異変　一刻も早く　報告を
少しでもおかしいと感じたら、一人で判断せず、
すぐに上司や担当者に報告しましょう。

サイバー攻撃等の脅威に対処するため、ルールを確立し、従業員間の共有を図り みんなで会社を守りましょう！

愛知県警察 AICHI POLICE