落合駐在所だより ～広報おちあい～ 令和7年 2月号

フィッシング詐欺にご注意

最近、インターネット上で、アカウント情報（ユーザーID、パスワード等）、クレジットカード番号、暗証番号等の重要な情報を盗み、本人になりすまして不正な取引を行う「フィッシング詐欺」の被害が多数発生しています。

○ フィッシング詐欺とは
銀行やクレジットカード会社、ショッピングサイト等の実在する企業を装った電子メールを送り、企業のホームページと酷似した偽物のWEBサイトに誘い込み、アカウント情報（ユーザーID、パスワード等）、クレジットカード番号、暗証番号等の重要な情報を盗み、本人になりすまして不正な取引を行う犯罪行為です。

※ フィッシング詐欺の被害に遭わないための対策
★ 個人情報やクレジットカード番号等を促す電子メールに注意する
銀行、クレジットカード会社やショッピングサイト等は、アカウント情報等について電子メールやSMS（ショートメッセージ）で問い合わせしたり、回答を促すようなことはありません。
★ 届いた電子メールのアドレスや本文に記載されているURLが正しいものか確認する
むやみに電子メールやSMSにリンクされたURLをクリックしないようにしてください。 → 公式アプリや公式サイトから確認しましょう。
★ パソコンやスマートフォンを安全に保つ
OSやアプリ、ソフトウェアのぜい弱性や不具合を悪用し、広告などからフィッシングサイトに誘導される場合があるので、OSやアプリ、ソフトウェアのアップデートを行い、パソコンやスマートフォンを安全な状態に保ってください。
★ IDやパスワード、クレジットカード番号等を管理する
IDやパスワード情報を盗まれた場合、他のWEBサイト等にアクセスされ、不正利用被害に遭うリスクが高くなります。
被害を抑えるためにも、IDやパスワードの使いまわしはせず、WEBサイトごとの情報を把握しておきましょう。
★ 携帯電話会社などが提供するセキュリティ設定を活用する
携帯電話会社などが提供する迷惑メッセージブロック機能などを活用し、フィッシングメールや不審なSMSが届きづらい設定にしてください。

冬のヒートショック予防

冬場などに、元気だったのにお風呂やトイレで亡くなっていたという話を聞いたことがありませんか？
「冬のお風呂の落とし穴！」ヒートショックにご注意ください。

○ ヒートショックとは
寒暖差によって血圧が急上昇・急降下することにより、血管や心臓に大きな負担がかかることを指します。
ヒートショックが発生すると、意識喪失や脳梗塞、心筋梗塞などが発生しやすくなり、死亡に至ることもあります。
とくに、浴室内での発生は、溺水に繋がる可能性があるため注意が必要です。
● 浴室での血圧変動の流れ
・ 暖かい部屋から寒い脱衣所へ→血管が縮み血圧上昇
・ 寒い脱衣所から熱いお湯につかる→血管が広がり血圧低下

※ 入浴についての注意点
★ 部屋間の温度差をなくす
脱衣所に暖房器具を設置し、入浴前に暖めましょう。
また、浴槽内にお湯がたまっている場合は、寒暖差をなくすため入浴前にふたを開けておきましょう。
★ お酒を飲むなら入浴後に
飲酒すると、血管が拡張して血圧が低下しますので、お風呂は飲酒前に入りましょう。
★ 浴槽の湯温を低めにする
41℃以下のあまり熱くないお湯に入りましょう。
★ 長湯をしない
お湯につかる時間は、10分までを目安にしましょう。
★ 浴槽から急に立ち上がらない
急に立ち上がると、めまいが起きることがありますので、浴槽から出るときは、手すりや浴槽の縁を持って、ゆっくり立ち上がりましょう。
ヒートショックは予防できますので、上記注意点を取り入れて健康で安全な生活を送ってください。

２月１日から３月１８日までは「サイバーセキュリティ月間」

● サイバーセキュリティ月間について
現在、パソコンやスマートフォンの普及により、誰でも簡単にインターネットや電子メールを利用できる環境にあります。
インターネットなどは便利な反面、サイバー攻撃の標的となる場合があります。
そこで政府では、ネットワーク（インターネット等）やモバイルデバイス（ノートパソコン、タブレット端末、スマートフォン等）の情報技術資産をサイバー攻撃から保護する取り組み、いわゆる「サイバーセキュリティ」を重点的かつ効果的に推進するため、２月１日から３月１８日までの間を「サイバーセキュリティ月間」と定めています。
● サイバー攻撃とは
サイバー攻撃とはインターネットやデジタル機器を使用し、サーバーやパソコン、スマートフォン等の情報端末に対し、システムの改ざんなどを行う行為です。
● サイバー攻撃の種類について
○ フィッシング詐欺
偽サイトに誘導され、クレジットカード番号や口座番号などを盗み取る詐欺
例 ・ 大手企業や銀行、クレジットカード会社を装ったメールなどで偽サイトに誘導する
・ ウイルス感染をうたって偽サイトに誘導する
○ ＤＤｏＳ攻撃
まず１台のパソコンを乗っ取り、そこから他の多数のパソコンに侵入、目的のＷｅｂサイトやサービスに大量の通信を発生させ、高負荷を与える攻撃
高負荷を与えられたＷｅｂサイトやサービスは利用停止となる
○ ランサムウェア
パソコン・サーバのデータを暗号化し、業務を停止させる
データの復元する代わりに身代金を要求する
● サイバーセキュリティ対策について
前段で紹介したサイバー攻撃はほんの一握りです、様々な種類のがあり、年々手口などが複雑、巧妙化されています、対策としては
○ ソフトウェアやＯＳを定期的にアップデートする
○ ウイルス対策ソフトを導入する
○ 強固なパスワード設定する
○ 不審なメールを開かない
○ 個人情報をデバイスに保存しない
○ 注意してＷｅｂサイトを閲覧する
などがあります。
● まとめ
パソコン、スマートフォンが身近になっているからこそ、各々が正しい知識を身につけ、自衛することが大切になっています。
「サイバーセキュリティ月間」の期間にご自身のセキュリティ対策を見直してみてはいかがでしょうか？

積雪・凍結時の事故防止

厳しい寒さが続いています、積雪・凍結対策されていますか？
毎年、積雪時は交通事故が多発します。
チェーンやスタッドレスタイヤなどの積雪対策をお願いいたします。
平地で雪が溶けた後でも山間部は注意が必要です。
日陰になっている場所はなかなか雪が溶けず、アイスバーンになっていることがあります。
また、積雪がなくても強い寒気が入ると路面凍結の恐れがありますので注意が必要です。
天気予報をこまめにチェックするなど早め早めに準備をして積雪・凍結に備えましょう。
☆ 四駆ならノーマルタイヤでも大丈夫？
「四輪駆動車は雪道に強い」「雪が降ってもノーマルタイヤで大丈夫」などと聞いたことはありませんか？
確かに四輪駆動車は構造上４本のタイヤに動力が伝わるため、二輪駆動の車と比べ雪道での安定感は勝ります。
しかし、だからと言って滑らないわけではありません、実際に四輪駆動車のスリップ事故も少なからず発生しています。
車両の安定性に差はあってもタイヤの性能が上がるわけではありませんので四輪駆動車に乗られている方も過信せず、スタッドレスタイヤ等の用意をお勧めします。
また、四輪駆動車は車両重量が重たいものが多く、他の車と比べて雪道での制動距離（ブレーキを踏んでから停車するまでの距離）が長くなるという実験結果もあるようです。

【落合駐在所管内】事件・事故発生状況

令和6年1月～12月（暫定値）

◎ 事　件　　なし
◎ 人身事故　3件
◎ 物件事故　21件