滋賀県警からのサイバーセキュリティに関するお知らせ

新型コロナウイルスの流行に付け入るサイバー犯罪多発
【継続】自粛後もセキュリティ対策を推進しましょう

新型コロナウイルス感染拡大による混乱に付け込もうとするサイバー犯罪が発生しています。

経営自粛によってテレワークの導入が多くの企業等で取り入れられたほか、インターネットを使った新たなサービスが提供されるなど、オンライン化が進み、今後も進展すると思われます。

オンライン化の進展によって利便性は高まりますが、同時に、不正アクセスや情報漏えいのリスクもありますので、セキュリティ対策を推進してください。

また滋賀県は緊急事態宣言が解除されましたが、新型コロナウイルス感染拡大に便乗したサイバー犯罪は日々の情勢に合わせて進化していますので、引き続き注意をお願いします。

「医療、製薬関係企業」がサイバー攻撃の対象に

治療薬やワクチンを研究、製造する機関や企業が世界規模でサイバー攻撃の対象となっています。

研究、製造に関連するサプライチェーン企業もサイバー攻撃を受けるおそれがありますので、出入り業者や下請け業者の方々も注意が必要です。

標的型攻撃メールによるマルウェア感染や情報流出に注意してください。

【ポイント】 メールの添付ファイルの開封や本文中の URL のアクセスは慎重に行いましょう。

給付金・助成金に関する詐欺メールに注意

持続化給付金等の給付金や助成金の対策に便乗した詐欺メールに注意してください。

また、行政機関を装った偽サイトが確認されており、こうした詐欺メールや偽サイトが増加する可能性があります。給付金や助成金に関する情報はよく確認するようにしてください。

【ポイント】 給付金に関する手続きや問合せは公式サイトで確認しましょう。
メール等に記載された URL にアクセスしないようにしましょう。

テレワーク終了時後のセキュリティ

テレワークによって職場のパソコンを家庭等で使用した場合は、家庭等で使ったネットワークにおいてウイルス感染しているおそれがあります。

必ずウイルスチェックを行ってから職場のネットワークに接続するようにしてください。

また、緊急的にテレワークを導入しオンラインによる業務を実施した場合は、セキュリティ対策が充分でない場合がありますので、セキュリティ対策を確認してください。

【ポイント】 外部のネットワークに接続したパソコンは必ずウイルスチェックを行いましょう。

[お知らせ] 情報発信は正確に。デマやフェイクニュースに注意しましょう。

滋賀県警察本部サイバー犯罪対策課 （代表）077-522-1231