スマホ決済を安全に利用しましょう

クレジットカードを始めとしたキャッシュレス決済の利用が増加し、最近はスマホ決済も多くのユーザーに使用されています。スマホ決済には、「非接触型決済」「QRコード決済」の2種類があり、それぞれ利用方法が異なります。

非接触型決済
（非接触IC決済）
非接触ICが搭載されたスマートフォンを店舗の読み取り機にタッチしたり、かざすだけで決済できます。

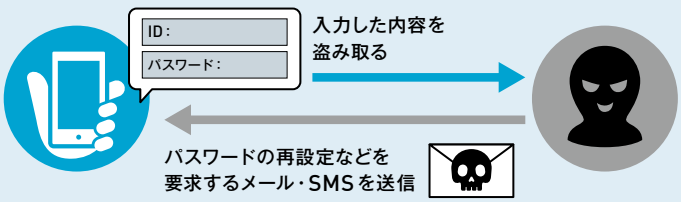
QRコード決済
スマートフォンにインストールしておいたアプリに表示されるQRコードやバーコードを店舗側が読み取ったり、店舗側が用意しているQRコードを自分のスマートフォンで読み取ってから金額を入力したりすることで決済できます。

ご注意ください！　スマホ決済サービス不正利用の要因！

スマホ決済の利用者が増加している一方で、サービスの不正利用も確認されています。
被害を未然に防ぐために不正利用の要因をご紹介します。

要因1　フィッシングによる決済サービスのID・パスワードの漏洩

犯罪者は、決済サービスのIDとパスワードを狙っています。メールやSMSを送信して、メッセージ内のURLリンクから受信者をフィッシングサイトへ誘導し、認証情報等の入力を求めます。そこで入力した情報は、全て犯罪者に知られてしまいます。



要因2　ID・パスワードの使い回し

犯罪者は、不正に入手したIDとパスワードをリスト化し、様々なサービスへのログインを試みます。同じIDとパスワードの組み合わせを複数のサービスで共有していると、決済サービスを含む各種サービスのアカウントを全て乗っ取られてしまう危険性があります。

要因3　決済アプリを入れているスマートフォンの紛失

紛失や盗難により、悪意のある第三者の手に渡ってしまうと、決済アプリを不正利用される可能性があります。

不正利用を防ぐためのチェックポイント

☑ チェック1 情報入力は慎重に	メールやSMS、Web広告などから誘導されたサイトでIDとパスワードの入力を求められた時は、正規のサイトかどうかをURLなどで確認しましょう。よく利用するサイトはブックマークに登録しておき、そこからアクセスしましょう。
☑ チェック2 ID・パスワード管理を厳重に	サービスごとに異なるIDとパスワードを使用しましょう。また二要素認証などを設定できる場合は必ず有効にしましょう。仮にパスワードが犯罪者に漏洩したとしても、アカウントの不正利用を阻止できる確率が高まります。
☑ チェック3 画面にロックを	スマートフォンには必ず画面ロックをかけましょう。ロック方式には、パスワードやパターン、指紋認証、顔認証などがあります。ロックを解除しなければスマートフォンを操作できないため、紛失、盗難時のセキュリティ対策になります。

※不審な取引を見つけたら…
スマホ決済の利用履歴を日頃からチェックしましょう。不審な取引を見つけた場合は、速やかにサービス提供事業者に連絡しましょう。

三重県警察本部生活安全部サイバー犯罪対策課
協力：三重サイバーセキュリティ・アイザック

MieCS-ISAC