



ライフサイクルに合わせた情報をお伝えいたします！



第12回 (管理編)

『インターネットアカウントについて』

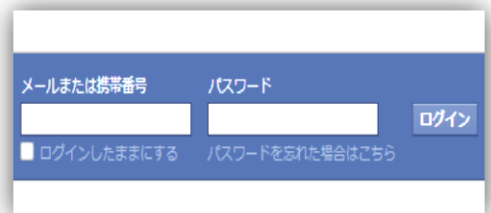
インターネットが普及し、もはや生活になくてはならない存在となり様々な企業が便利なサービスを提供しています。TwitterやFacebook・LINEなどのコミュニケーションサービスや、インターネットバンキングや通販サイトなどもスマートフォンからアクセスしやすくなりました。ところがそれらの便利なサービスを利用するときに必ず必要なものがあります。それがログインするとき使用するアカウントです。今回はそのアカウントの危険性についてご紹介したいとおもいます。

インターネットアカウントの危険性って？

皆

さんFacebookを使うときに「ログイン」ってしますよね。

Amazonで買い物をするときも「サインイン」を行います。名前は違いますがやっていることは同じです。ログインをすると自分の個人情報が見れるようになったり、購入履歴やクレジットカード情報などを確認することができます。



アカウントサービス

Would you like to see this page in English? [Click here.](#)

注文履歴

注文内容の確認または変更



注文内容の確認、変更はこちらから

[注文履歴を見る](#)

注文履歴

未発送の注文を見る

支払い方法の設定

クレジットカード・Amazonギフト券

お支払い方法について

クレジットカード情報を編集・削除する
クレジットカードを追加する
マイポイント(Amazonポイントの獲得・利用履歴)を確認する
パートナーポイントを管理する

も

しこの情報が他人に知られてしまったら・・・

とんでもないことになりますよね？ Amazonで勝手に商品を購入されたり、口座からお金を引き落とされたりしてしまいます。今回はそのとんでもないことになってしまった事例と対処法をご紹介します。

こ

ちらの画面、皆さん見慣れていると思います。

LINEのトーク画面ですが、少し変ですね。実はこの会話の相手側は、私の友人だったのですがLINEのアカウントを乗っ取られてしまいました。

アカウントを乗っ取った攻撃者は、登録されている友人に片っ端から「webマネーが急ぎで必要です」などと送りシリアルを写真で撮って送るよう指示できます。そして何も知らない人は騙されて指示通りに送金してしまうのです。



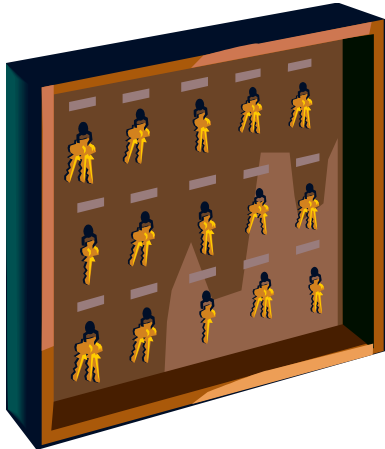
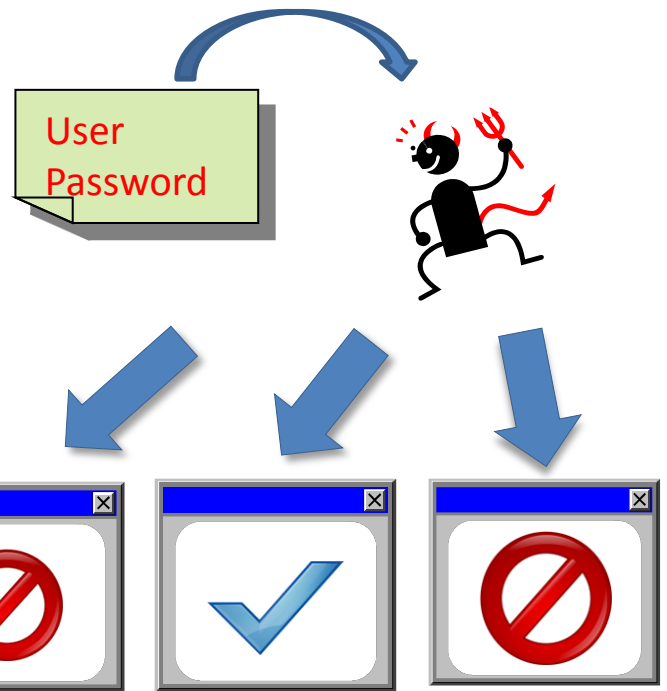
悪意のあるユーザーはどうやってこのようなこと

ができるのか、実はこのアカウント乗っ取りにはタネがあります。

皆さんGoogleやYahoo、Amazon、Twitterなど様々なサービスに登録されていると思いますが、「ユーザー名」と「パスワード」を使いまわしてはいませんか？

悪意のあるユーザーはアカウント情報を入手するとその情報で様々なサイトにアクセスしようとします。そしてユーザー名やパスワードを使いまわしていると別のサイトでログインが成功してしまうのです。

これを『リスト型攻撃』といいます。



か

とってユーザー名とパスワードを使いまわさないようにできるのか、
というところでもありません。

今やネットワークアカウントは1人最低5個は所持しています。多い人だと数十個にも上ります。それらのアカウントでユーザー名とパスワードをバラバラにして覚えていられる人はそうそういません。

そこで『パスワード管理アプリ』が登場してきます。すでにスマートフォンのアプリで多くの種類が普及しています。そのアプリに各サイトのユーザー名とパスワードを記録しておき、閲覧するためのパスワード1個を覚えておけば何十個もの情報を覚える必要はありません。

イメージとしては「キーボックス」です。キーボックスの鍵を持っていればボックスの中の鍵を取ることができます。

最後にアプリの紹介QRコードを記載しますので、興味のある方は一読をしてみてください。

今年の6月にMixiやLINE、ニコニコ動画などの有名サイトで情報が流出し、リスト型攻撃の被害者が続出しています。7月にもベネッセの情報流出事件があり、個人情報漏えいしています。更なる被害を防ぐためには、企業だけではなくサービスを利用する私たちにも、情報に対するリテラシーが必要です。



ぱすわ〜ど帳
(android用)



RoboForm



パスワード金庫Lite
(iPhone用)