

Facebook

スパムから身を守って 他人に優しくして 熟睡するための方法

目次

素敵な挨拶	2
まず最低限やってほしいこと	3
セキュア接続	
モバイル設定	
ログイン承認	
ログイン通知	
友達が使ってるスパムアプリから自分を守る設定	4
それスパム！と言われたり何かやっちゃったかなと感じた後の対応	5
アカウントが乗っ取られたなーと思ったら	5
その他にやっておいた方（知っておいた方）がいい設定	6

■ 誰だって最初はわからん

せっかくFacebookを楽しもうと思って始めたのに、スパムだかスカムだか何だかよくわからないものに騙されて「**それスパムだよ!**」って言うてる方もそれが何だか良く分からないんだけど「悪いもの」っていう認識はある。アワワウっていう間に「スパムを踏むような情弱とは縁を切れ」なんて何だかすごい正義らしい言葉が舞い降りてきて「そーなの? そーなの? 私は悪なの?」

なんて世界がいいわけない!

■ 怖くてもうFacebookに触りたくない

スパムだかスカムだかフィッシングだか分からないけど、怖くてFacebookに触りたくないってことにもなるし、実際にスパム踏んだだけでアカウント消しちゃう人まで。それは本人が悪いっていう声がかいけど、周りが悪い。ゆるそーよ、それくらい。

っていう考えがあってもいいと思わないっすか?

■ 結論から 設定ガイド

もう、めんどくさいことはどうでもいい。とにかく何も考えず大事なことだけ教えて、という声が聞こえそうな気がするので行くぜ!

ちなみにFacebookページのオーナーさんもこれらの設定は必須。

説明が下手だから、分かりづらいところはむしゃむしゃ咀嚼しないで読飛ばして。でも、設定だけはこのままやっておくのがいいっすよ。

■まず最低限やってほしいこと

1.セキュア接続

一番最初にやって欲しいこと。

<https://www.facebook.com/settings?tab=security>

セキュリティ設定

セキュア接続	<input checked="" type="checkbox"/> セキュアな接続(https)を利用する(可能な場合)	
	<input type="button" value="変更を保存"/> <input type="button" value="キャンセル"/>	
ログイン通知	メールによるお知らせがオンになっています。	編集
ログイン承認	未認定機器からログインした場合の承認は現在必須に設定されています。	編集

デフォルトではオフになっているセキュア接続。これをオン！チェックボックスにチェックを入れて変更を保存する。暗号化されていないセッション、WEBアプリの使用などでアカウントが乗っ取られる被害を小さくする。未だにセキュア接続未対応のタブページなどがある。必要でないなら設定解除してまで見る必要なし。

2.モバイル設定

<https://www.facebook.com/settings?tab=mobile>

「(別の) 携帯電話番号を追加」をクリック。ここで入力するパスワードはFacebookにログインする時に使っているもの。「承認」ボタン。その後立ち上がったウインドウに電話番号を入力。その際、キャリアによって電話番号を受け付けてもらえないことがある。正しい番号を入れるように、と促された場合はキャリアから配布されているメールアドレスを入力。国は「日本 (+81)」を選択。その後、指定のメールかSMSで確認コードが送られてくるので、ブラウザの入力フォームにそのままを入力して設定完了。確認は取れていないが、音声による通知の可能性もあるので心の準備を（SMSの受信を拒否する設定をしていないかチェックしてから進める。メールの受信設定も気をつけてね）。

3.ログイン承認

<https://www.facebook.com/settings?tab=security>

「未認定機器からログインする場合、セキュリティコードの入力を要求する」にチェックして「変更を保存」。普段自分が使用しているパソコンのブラウザ単位、スマートフォンのアプリやブラウザ単位でログイン可能な環境を限定できる。誰かが不正にログインすることができなくなる。ただし、ネットカフェなどを頻繁に利用する人には向かない設定。でも、不特定多数が利用するデバイスを使ってログインする必要のあるサービスは利用しない方がいい。

4.ログイン通知

上記の流れから、ひとつ上にある「ログイン通知」のメールアドレスにチェックして「変更を保存」。ここまでで一段落。誰かがあなたのログイン情報を入手する可能性は今までよりも低く、仮に盗まれてもログインされる確率はものすごく下がった。**つまり、だいぶ安全になったよ！**

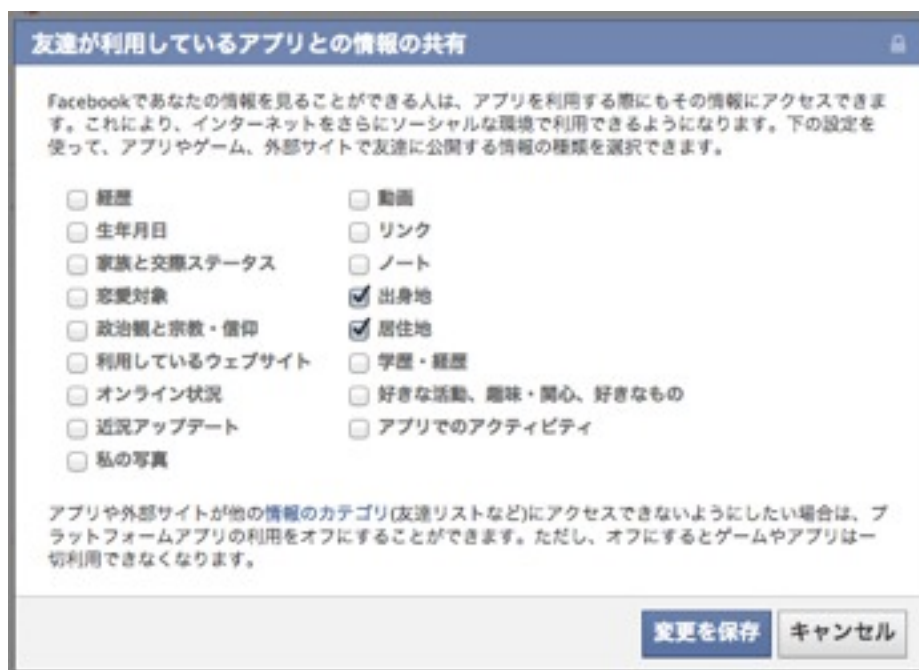
ただ、最初のうちはちょっと不便なこともある。普段使っているパソコンでも設定時に使用したブラウザ以外でアクセスしようとしても「未登録」なので確認用コードを入れると言われる。そんな時は、モバイル設定で登録した携帯電話にコードが送られてくるからそれをちょいちょいと入れてあげればOK！デバイスに名前をつけろと言われるけど、好きな名前をつけたらいいさ。例えばMBAのChromeとか、PC Firefoxとか、そんな感じで。

ログイン承認した端末は「認証済み機器」から確認が可能。心当たりのないものがあたら恐らくそれは単なる物忘れだと思うが念のために削除しておこう。もし自分が登録した物で今後もログインに使う端末なら次のログインにまた登録しておけばいい。安全に使う設定は後もう少し。あとちょっとだけ張り切ってほしい。

■ 友達が使ってるスパムアプリから自分を守る設定

<https://www.facebook.com/settings/?tab=privacy§ion=apps&h=AQMwdlb7PVoEOwmb>

他のユーザーが利用しているアプリとの情報の共有、を「編集」をクリックするとこのウィンドウが立ち上がる。



友達に公開している情報って結構ある。誕生日とか、経歴なんかも含めて通常の投稿も。で、その友達が使ってるアプリがその公開されてる情報を持ってってしまうこともある。あなたとしてみれば友達にだけ見せるつもりでも、いったん友達に渡った情報はあなたの個人情報で

Facebookのスパムから身を守ろう

あっても、煮るのも焼くのも売るのも友達の自由だ。モラルを持ち出しても意味がない。それがいやなら自衛する。

というわけで、渡したくない情報はチェックを外す。渡してもいいやと思えるものはチェックを残して「変更を保存」。もちろん全部外してもOKよ

■ それスパム！と言われたり何かやっちゃったかなと感じた後の対応

・ アプリの削除

慌ててアカウントを削除する必要なんてない！「この情弱やろう！」と罵られたら、こちらから先に友達解除する位でOK!

<https://www.facebook.com/settings/?tab=applications>

ここから「スパム！」と言われたアプリとか見慣れないアプリを削除してしまおう。右側にある×をクリックして削除。

・ パスワードの変更

気持ちは分かるのだけど、他のサービスで使用しているパスワードを使用するのは危険。決済サービスまで他のサービスと同様のパスワードを使っているのは「どうぞ盗んでください」と言ってるようなもの。簡単すぎず、それぞれに統一性がなくて忘れてしまったりということがないようにしたい。

便利なパスワード管理ツールなどもあるので参考にされたし。

<http://www.lifehacker.jp/2010/05/100512password5.html>

Facebookのパスワード変更は

<https://www.facebook.com/settings?tab=account>

から「パスワード」

■ アカウントが乗っ取られたなーと思ったら

<https://www.facebook.com/help/?faq=203305893040179#アカウントがハッキングされました。>

から報告。↑うそみたいなURLだけど、本当だから安心して

■ その他にやっておいた方（知っておいた方）がいい設定

必ずしもセキュリティに関係しなくても知っておいた方がよい設定をいくつか

・ ユーザーネーム（ユニークURL）

facebook.com/の後に任意の文字列を設定しておく覚えやすいし名刺にも印刷することもできる。当然早い者勝ち。

<https://www.facebook.com/settings?tab=account>

・ Facebook上の自分の活動データを取得

Facebook上でシェアした写真、動画、ウォール投稿、メッセージ、チャット履歴友達の名前などのデータをダウンロードすることが可能。上記URLの最下部「Facebookデータをダウンロード」

・ 退会

<https://www.facebook.com/settings?tab=security>

の最下部「アカウントの利用解除」から。

・ フィード購読設定

<https://www.facebook.com/settings?tab=subscribers>

「フィード購読を許可」しておこう。そうしないとうるさい友達リクエストに悩まされる可能性が高くなる。

・ タグ付けされることの許可設定

<https://www.facebook.com/settings/?tab=privacy>



取引先に嘘をついて都合を調整して参加した飲み会。そこで写真にタグ付けされて勝手に投稿されたたまらん。現場で「タグ付けはやめれ！」と言い切れない雰囲気もある。そんな時はこんな設定で乗り切るべし。上記URLから「タイムラインとタグ付け」の「設定を編集」
大事なのは上記赤で囲んだ二つの項目。要するに勝手にタグ付けして、自分が知らない間にタイムラインに掲載されて写真などが流出したり、いるはずのない場所にいることにされたりすることを防ぐ設定。他項目の設定は詳細は省略するけど、上記オススメパターン。

・進行中のセッション

<https://www.facebook.com/settings?tab=security§ion=sessions&view>

今アクセスしている環境が表示される。まったく見覚えのないアクセスがあるなら「終了」でセッションを終了させてしまおう。

・お知らせの設定

<https://www.facebook.com/settings?tab=notifications>

Facebookからのメールの通知がうるさ過ぎる、と感じているならページ上部右側の「メールの頻度：ここのお知らせメールではなく、（略）」にチェック。重要なグループや管理しているページのアップデートのお知らせを個別に設定したい場合は逆にチェックを外して各項目を設定。

・アクティビティのログ

<https://www.facebook.com/>（個人のユーザーネーム）/allactivity

自分がいいね！したりコメントしたりした投稿を後でまとめてみれます。いいね！をメモ代わりに使えるので便利。でも、多用しすぎると、あなたのいいね！の価値が低下するので注意（あいつのいいね！や安い、と言われることも）。

Facebookのスパムから身を守ろう

書き手：栄花均（ソーシャルメディアストラテジスト）

Facebookページもあるよ。いいね！してね

<https://www.facebook.com/thinking.scl>

ソーシャルメディアの正しい活用ならお任せ

WEBOSS株式会社：

<http://www.weboss.jp/>

札幌市中央区南2条東2丁目9番地

大都ビル4階

011-271-6466

この資料の引用、再配布など特に制限しませんが、出典明記していただければ幸いです。