

ホームページにメールアドレスを掲載すると詐欺メールが多く来る。

google などはロボット(目的を実行するプログラム)を使って自動的にリンクをたどって WEB ページを探し、言葉のリスト化を行う

詐欺メールの発信者は同様に文字列+@+文字列(もっとメールアドレスとわかる条件で絞り込みをしているかもしれない)を使って検索し、リスト化する。→このリストに基づいてメールを発信する。(エラーで返ってくるものはリストから外すかもしれない)

対策

ホームページにメールアドレスを載せるときわざと@の前と後を切り離す @を(at)等 に置き換え、メールを打つときは@に読み替えてくださいと注をいれる→ あまり これが一般化すると、これを検索するロボットをつくるかもしれない

イメージで掲載する。→イメージを読み取るロボットを作ることも不可能ではないが面倒

現役のときの公用メールアドレス

外部との連絡

客がアポをとるため連絡してくるときは電話 またはメール

電話はそのままホームページに載せるがメールアドレスは@以下のドメイン名は組織共通にして別の個所に掲載し@の前だけ個人別に表示

電話 不在の時つながらない セールス電話が良くくる。今は引退しているから知らない電話には出ないまたは留守電にする。現役時には知らない番号でも電話をとる必要があった。

メール 相手がメールアドレスをすべて打ち込む必要があったがやむをえない

個人メールアドレス

インターネットに加入 鎌倉ケーブルテレビ

メールアドレス aono@kamakuranet.ne.jp

鎌倉ケーブルテレビが JCN を経て JCOM に統合

新メールアドレスの設定が必要

aono@jcom.zaq.ne.jp を選択

新しいメールアドレスの設定を示されたとき、即今のアドレスを設定 早いもの勝ちでシンプルなアドレスを獲得できて満足→アサハカであった。

aono は tanaka、sato 程よくある苗字でないが、数百位以内に入るシンプルな苗字 迷惑メールのアドレスで作られやすい 月に 1~2 件 Aono+ランダムな数値にしておけば良かった

半月ほど前にきた気分が悪くなるメールの例(年数回くる) 英文でも来る

「こんにちは！

残念ながら凶報がございます。

数ヶ月前、あなたがインターネット閲覧に利用しているデバイスへのアクセス権を取得しました。さらに、あなたのインターネット活動の追跡も行いました。下記は、それまでに至る経緯です。

以前、ハッカーから複数のメールアドレスへのアクセス権を購入しました(最近では、オンライン上で簡単に購入することが可能です)。

よって苦勞することなく、あなたのメールアカウント（aono@jcom.zaq.ne.jp）にログインしています。

あなたのデバイスにアクセスしてから1週間以内に、メールに利用されているデバイスのオペレーティングシステム全てにトロイの木馬ウイルスをインストールしました。

実際、この操作はかなり単純です（なぜなら、あなたが受信メールをクリックしたからです）。

中略

この件は下記のように解決させましょう。

あなたがすべきことは、ただ ¥200000 を私のアカウントに送金するだけです（送金時の為替レートに基づくビットコイン相当）。送金が完了すると、私はすぐに全てを削除します

後略」

1ヶ月に1~2件なので、それほど負担にならないが、気分が悪い 発信元のメールアドレスも偽装している。（自分自身から送ったように装っている）→発信元メールアドレスで迷惑メールに分類することができない→本文に「トロイの木馬ウイルスをインストール」で分類→迷惑メールで分類 で様子見

クレジットカード

現役時代はクレジットカードの利用はほとんどなし

1円単位の端数処理が面倒で徐々に利用増加

高額な買い物やレストラン利用のとき、カードをスタッフに預ける方式→経験がないことはないが、基本的に預けることはしない←番号を読み取られる恐れ

オンラインでクレジットカード番号のみで買い物ができる。信頼性に不安 伝送途中は漏洩が守られても少なくとも相手には番号がわかる。

クレジットカードマスターという手法あり→番号をでたらめに入力しヒットすれば使える番号として悪用する。→クレジットカード番号にはある程度の規則性あり。全くランダムというわけでない。→ユーザとして防ぐ方法はない

毎回利用明細を確認し、覚えのないものはクレジット会社に通報するしか方法はない

SUICA

極めて便利

ただし使用した履歴がわからない(と最近までは思っていた)

時々計算が合わなくなるときあり

PayPayなどの即時決済の方式は手間が省けて便利だが手元控と実績が合わなくなったとき原因追及が面倒(と思ってまだ利用していない)