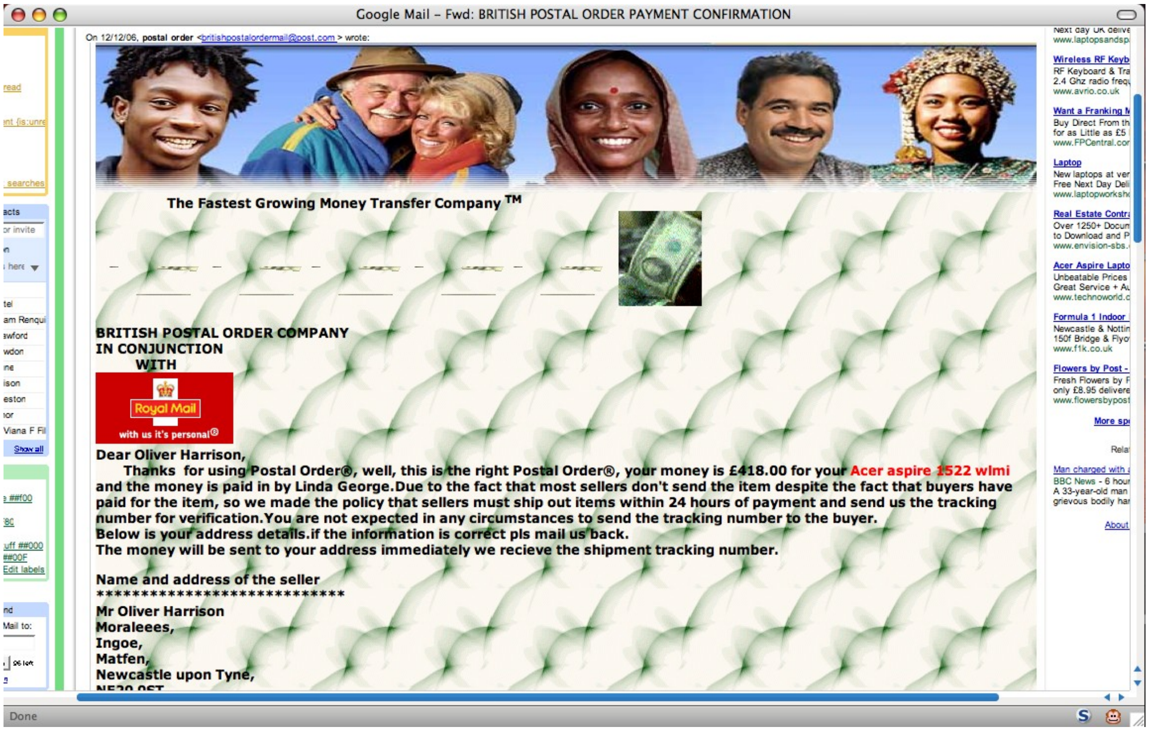
# Threats to data

People who use online sites shops a lot will know of the many threats to personal data, although online fraud does not always start online. Identity theft can be put to best use on the Internet. If someone was to get your credit card details, they would most likely use it on the Internet.

The main way to get someone information is using a Phishing scam, this is where the person is sent an e-mail from "their bank" or another commerce company claiming that their information is at risk or that they need to update their information

Another common scam is to target a reputable site, like eBay and buy an item up for sale and to trick the seller to send the item whilst faking a form of payment. I am going to go into this scam in more detail:



On 12/12/06, postal order <britishpostalordermail@post.com> wrote:

The Fastest Growing Money Transfer Company ™

BRITISH POSTAL ORDER COMPANY
IN CONJUNCTION
WITH

Royal Mail
with us it's personal®

Dear Oliver Harrison,
Thanks for using Postal Order®, well, this is the right Postal Order®, your money is £418.00 for your Acer aspire 1522 wlmi and the money is paid in by Linda George.Due to the fact that most sellers don't send the item despite the fact that buyers have paid for the item, so we made the policy that sellers must ship out items within 24 hours of payment and send us the tracking number for verification.You are not expected in any circumstances to send the tracking number to the buyer.
Below is your address details.if the information is correct pls mail us back.
The money will be sent to your address immediately we recieve the shipment tracking number.

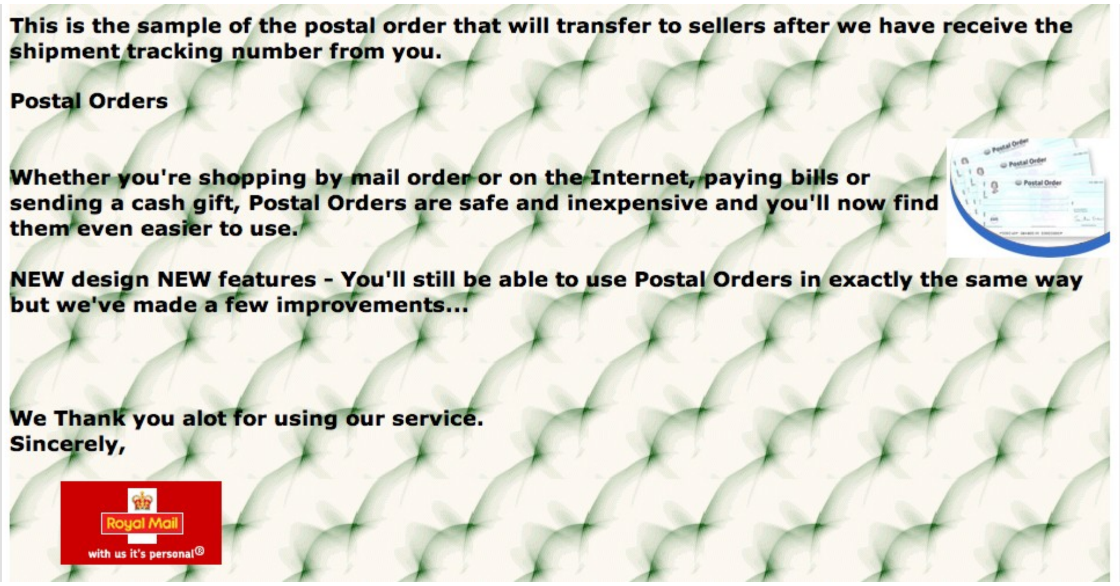
Name and address of the seller
***************************
Mr Oliver Harrison
Moraleees,
Ingoe,
Matfen,
Newcastle upon Tyne,

*Illustration 1: A con email trying to get someone to believe they are getting paid*

A quick glance at this particular email, and everything looks normal, but on closer inspection, there are a few errors:

- The first paragraph doesn't make sense: “well, this is the right Postal Order®, your money is £418.00”
- The use of “British Postal Order Company”, the Postal Order is a service provided by the post-office and is NOT a standalone Company.
- A google search for the catch phrase “The Fastest Growing Money Transfer Company” brings up another different money transfer company called “iKobo”

- The use of SMS language (e.g. Pls – Please)
- The use of animated clip art, all of the pictures on that particular email were hot linked from different sites on the internet.
- Later on in the email, the following occurs:



**This is the sample of the postal order that will transfer to sellers after we have receive the shipment tracking number from you.**

**Postal Orders**

**Whether you're shopping by mail order or on the Internet, paying bills or sending a cash gift, Postal Orders are safe and inexpensive and you'll now find them even easier to use.**

**NEW design NEW features - You'll still be able to use Postal Orders in exactly the same way but we've made a few improvements...**

**We Thank you alot for using our service.**
**Sincerely,**

*Illustration 2: The end of the email with a rather dubious statement*

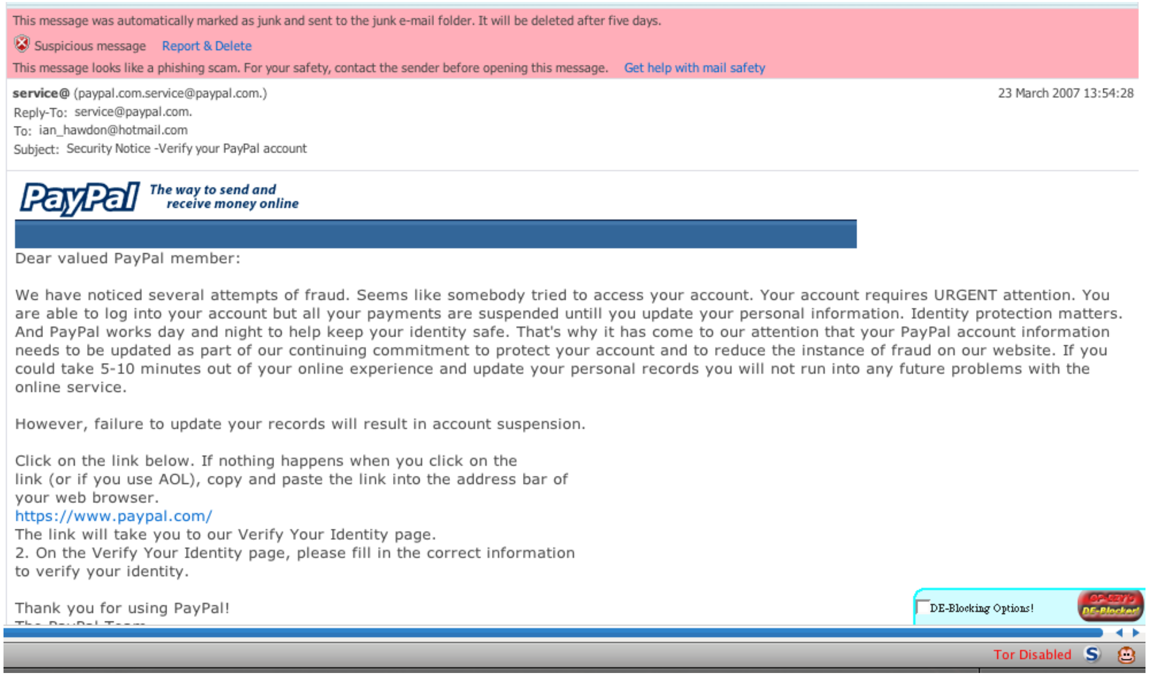
This email instructs the victim to send the item to receive a tracking number, then instructs them to reply to the email with that tracking number then they will ***send*** the money. The biggest risk with this is that the item has to be on its way before you can get the tracking number. This technically means that they will have the item, and no longer have to send any money.

- And the final point is that on the post-office website it clearly says:

WARNING: Please note that there are currently some Postal Orders scams being perpetrated - particularly on online auction sites. Please note that under no circumstances would Royal Mail or the Post Office™ issue an email notification of receipt of a Postal Order to a potential recipient. Should you receive such a notification, please report it to the police.

This shows that that email was clearly a threat to data and money.

The biggest problem is a full blown Phishing attack, in which the victim is tricked into giving away their personal details, I personally received one of these just today:



This message was automatically marked as junk and sent to the junk e-mail folder. It will be deleted after five days.

Suspicious message Report & Delete

This message looks like a phishing scam. For your safety, contact the sender before opening this message. Get help with mail safety

**service@** (paypal.com.service@paypal.com.) 23 March 2007 13:54:28
Reply-To: service@paypal.com.
To: ian_hawdon@hotmail.com
Subject: Security Notice -Verify your PayPal account

PayPal The way to send and receive money online

Dear valued PayPal member:

We have noticed several attempts of fraud. Seems like somebody tried to access your account. Your account requires URGENT attention. You are able to log into your account but all your payments are suspended untill you update your personal information. Identity protection matters. And PayPal works day and night to help keep your identity safe. That's why it has come to our attention that your PayPal account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension.

Click on the link below. If nothing happens when you click on the
link (or if you use AOL), copy and paste the link into the address bar of
your web browser.
https://www.paypal.com/
The link will take you to our Verify Your Identity page.
2. On the Verify Your Identity page, please fill in the correct information
to verify your identity.

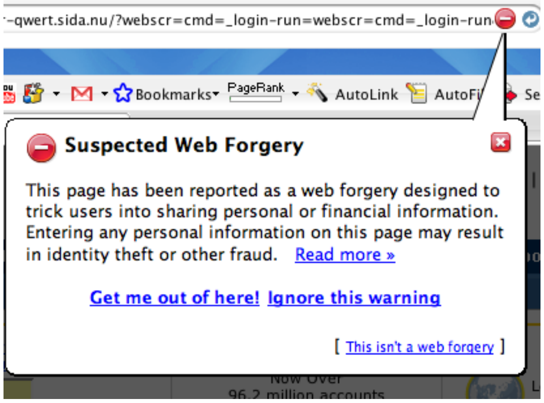
Thank you for using PayPal!
The PayPal Team

*Illustration 3: The email marked as suspicious*

As you can see, this particular email service (HoTMaiL/Windows Live Mail) identifies it as a phishing email and has advised me not to open it. I open it for the purpose of this essay. It should be also noted, that AOL users would be safe from this scam as it has instructions to copy and past the link (which in this case is the legitimate site link)

A few other things would also lead me to think this is a scam: The text continues beyond the picture logo across the top, my PayPal account is not registered to that email address and the email was in my Junk folder.

When the link is clicked, the victim's browser may splash a warning smiler to this one:



**Suspected Web Forgery**

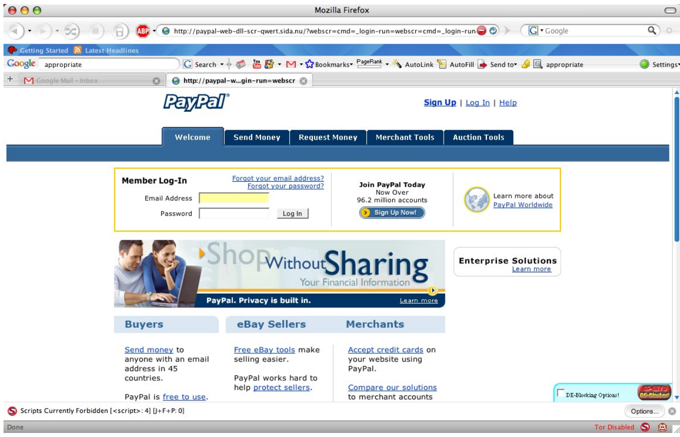
This page has been reported as a web forgery designed to trick users into sharing personal or financial information. Entering any personal information on this page may result in identity theft or other fraud. Read more »

Get me out of here! Ignore this warning

[ This isn't a web forgery ]

*Illustration 4: Mozilla Firefox 2.0.0.3 warning me of a forged page*

Although, once again, for the purpose of this essay, I clicked "Ignore this warning", this led me to the forged page. Here it is compared to the real PayPal site:


Mozilla Firefox

http://paypal-web-dll-scr-qwert.sida.nu/?webscr=cmd=_login-run=webscr=cmd=_login-run

Sign Up | Log In | Help

Welcome | Send Money | Request Money | Merchant Tools | Auction Tools

Member Log-In
Forgot your email address?
Forgot your password?
Email Address
Password
Log In

Join PayPal Today
Now Over
96.2 million accounts
Sign Up Now!

Learn more about PayPal Worldwide

Shop Without Sharing Your Financial Information
PayPal. Privacy is built in. Learn more

Enterprise Solutions
Learn more

Buyers: Send money to anyone with an email address in 45 countries. PayPal is free to use.

eBay Sellers: Free eBay tools make selling easier. PayPal works hard to help protect sellers.

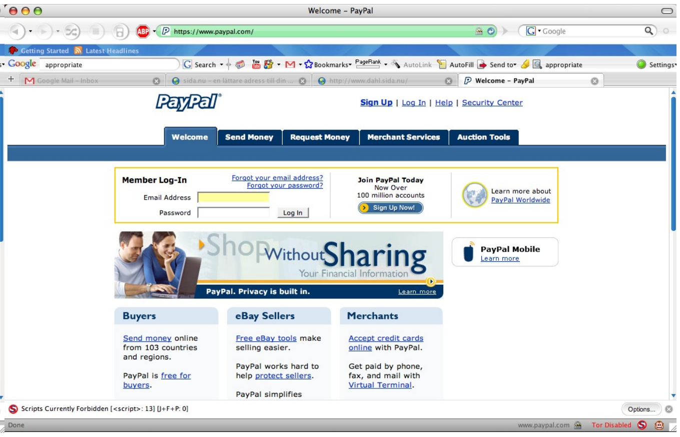
Merchants: Accept credit cards on your website using PayPal. Compare our solutions to merchant accounts

Scripts Currently Forbidden [<script>: 4] [J+F+P: 0]

Done

Tor Disabled

Illustration 5: The forgery


Welcome – PayPal

https://www.paypal.com/

Sign Up | Log In | Help | Security Center

Welcome | Send Money | Request Money | Merchant Services | Auction Tools

Member Log-In
Forgot your email address?
Forgot your password?
Email Address
Password
Log In

Join PayPal Today
Now Over
100 million accounts
Sign Up Now!

Learn more about PayPal Worldwide

Shop Without Sharing Your Financial Information
PayPal. Privacy is built in. Learn more

PayPal Mobile
Learn more

Buyers: Send money online from 103 countries and regions. PayPal is free for buyers.

eBay Sellers: Free eBay tools make selling easier. PayPal works hard to help protect sellers. PayPal simplifies

Merchants: Accept credit cards online with PayPal. Get paid by phone, fax, and mail with Virtual Terminal.

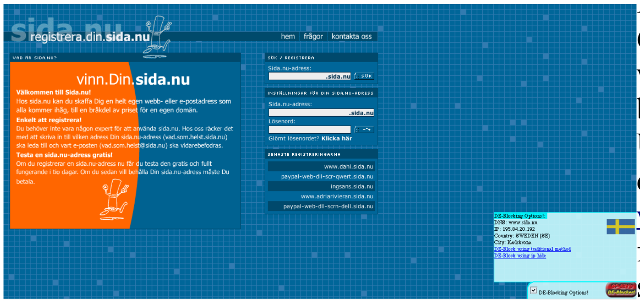
Scripts Currently Forbidden [<script>: 13] [J+F+P: 0]

Done

www.paypal.com

Tor Disabled

Illustration 6: The real PayPal site


registrera.din.sida.nu

hem | frågor | kontakta oss

VAD ÄR SIDA.NU?

vinn.Din.sida.nu

Välkommen till Sida.nu!
Hos sida.nu kan du skaffa Dig en helt egen webb- eller e-postadress som alla kommer ihåg, till en bråkdel av priset för en egen domän.

Enkelt att registrera!
Du behöver inte vara någon expert för att använda sida.nu. Hos oss räcker det med att skriva in till vilken adress Din sida.nu-adress (vad.som.helst.sida.nu) ska leda till och vart e-posten (vad.som.helst@sida.nu) ska vidarebefodras.

Testa en sida.nu-adress gratis!
Om du registrerar en sida.nu-adress nu får du testa den gratis och fullt fungerande i tio dagar. Om du sedan vill behålla Din sida.nu-adress måste Du betala.

SÖK / REGISTRERA
Sida.nu-adress: .sida.nu SÖK

INSTÄLLNINGAR FÖR DIN SIDA.NU-ADRESS
Sida.nu-adress: .sida.nu
Lösenord:
Glömt lösenordet? Klicka här

SENASTE REGISTRERINGARNA
www.dahl.sida.nu
paypal-web-dll-scr-qwert.sida.nu
ingsans.sida.nu
www.adriarivieran.sida.nu
paypal-web-dll-scrn-dell.sida.nu

DE-Blocking Options!:
DNS: www.sida.nu
IP: 195.84.20.192
Country: SWEDEN (SE)
City: Karlskrona
DE-Block using traditional method
DE-Block using ip hide

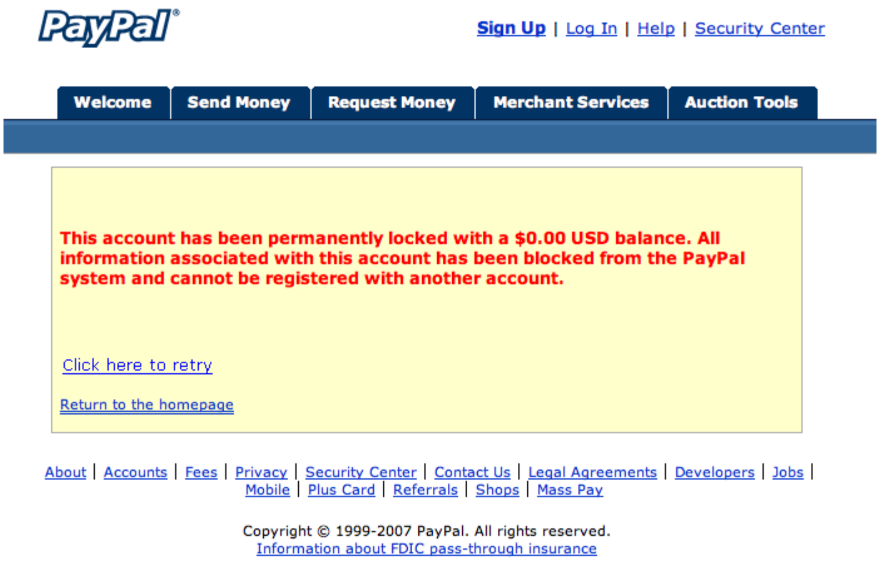
☑ DE-Blocking Options!

Illustration 7: Innocent sites get the blame for internet misuse

Illustration 5 shows the forged site, and 6 shows the real one, there are a few ways to tell the differences (if the web browser doesn't warn you), firstly, the URL in the forge tells us that the site's domain name is a subdomain from www.sida.nu. Sida.nu is a website, from Sweden, that provided subdomains to shorten long URLs, but some people use them to mask their site to make it look like an official companies site, to try and trick people to handing over their personal details.

The main page of SIDA.nu shows the latest 5 registered subdomains, 2 of which are PayPal scams and one of those no longer work. The phishing site itself is hosted in the USA at the site axdshipp.com. A DNS search for that site says that that site is hosed by www.andhosting.com

When the user puts his/her details into the fake PayPal website, the site will then claim that the details were incorrect and would have to be retyped. This is a common trick to make the person retype their details, confirming that their details are correct. It will then say that the information is incorrect again. If the victim still hasn't figured out that the site is a fake, they would click on the “forgot password” link. To avoid the loss of the freshly harvested password, the forgot password page is also from the forged site (as opposed to other pages that link directly to the real PayPal site). This page is will ask for the email address (confirming it for another time) and asks for a verification code (that is not checked), after this, the victim is greeted with this page:


PayPal
Sign Up | Log In | Help | Security Center
Welcome
Send Money
Request Money
Merchant Services
Auction Tools
About | Accounts | Fees | Privacy | Security Center | Contact Us | Legal Agreements | Developers | Jobs | Mobile | Plus Card | Referrals | Shops | Mass Pay

**This account has been permanently locked with a $0.00 USD balance. All information associated with this account has been blocked from the PayPal system and cannot be registered with another account.**

Click here to retry

Return to the homepage

Copyright © 1999-2007 PayPal. All rights reserved.
Information about FDIC pass-through insurance

*Illustration 8: A fake failing page*

But a threat to data does not just mean a scam to get people's personal details. The victim doesn't even have to have any participation in the attackers plan to get their details, for instance, if a worker at you "secure company of your choice" knows it is his last day at his particular workplace. He could get the user names and passwords to gain access to the secure information.

System problems can also cause problems and threats to data, if there is a power failure at some "high up" servers, data will most likely be inaccessible unless there is a mirror service set up, or the data may even be destroyed if the medium it was on wasn't cleanly unmounted during the power outage. Of course it doesn't just have to be power outages, fire, water damage, earthquakes also can cause problems.

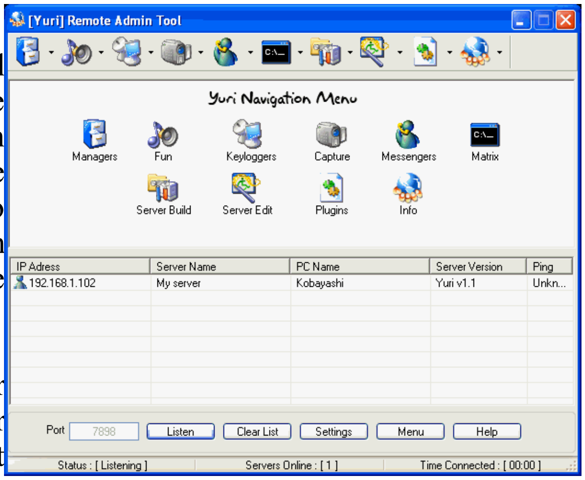
*"As usual, it can only be attributed to human error, Dave."* - HAL 9000.

Another problem is a hole in the system code, by an error on the programmers part. This means that other peoples data can be viewed by someone else, whether it is by accident or by some attacker.

A lot of attacks are done outside of the business that is being targeted.

- ➔ Hackers
  - o Non-Malicious – These are the people (usually students) who just want to hack into big businesses just to prove that it can be done. These people will not use the accounts that they find (Thus Non Malicious)
  - o Malicious – These people will hack the site for the purpose of:
    - ■ Vandalism – to either edit or destroy data, this means that the customer would have to re-enter their details, the hacker my even delete your account. Usually, the big company will have a backup of your data.
    - ■ Identity Theft – The hacker doesn't hack to vandalise, instead, they will find out your details, then use them to get your other details, or buy stuff from sites in your name.

Virus or other malware, allows someone to find out your information directly from your computer, viruses also can delete things. The ones that can steal data and take control of your computer are called Trojan Horses. A good example of a Trojan Horse is a program called Yuri RAT:



| IP Adress | Server Name | PC Name | Server Version | Ping |
|---|---|---|---|---|
| 192.168.1.102 | My server | Kobayashi | Yuri v1.1 | Unkn... |

Port 7898

Status : [ Listening ] Servers Online : [ 1 ] Time Connected : [ 00:00 ]

*Illustration 9: Yuri RAT, a Trojan Horse that performs many tasks*

Yuri Remote Admin Tool, to give it its full name, is a trojan horse that allows the attacker to look through the files on someone's computer, view what they type using a key logger, and allows them to scare the user by making the text to speech function in Windows XP say things to the user sitting in front of the computer.

The admin tool has to create a server program, that allows the victim's computer to talk to it. The server program must contain the IP address or domain name for information to be sent to and a port number for the client (the Yuri program) to listen to. The server program uses a masking name technique to trick the victim to run it, it could either be called msnmsger.exe (MSN Messenger) or iexplorer.exe (Internet Explorer). This means when the user presses CTRL + ALT + DEL to load task manager, and select the processes tab, there will be nothing that catches their eye in the list. Although, the server program does take up quite a bit of system memory, and can slow the PC that is running it.

Then there is the Denial of Service attack (or DoS [not to be confused with the text based Disk Operating System]), a DoS attack is when a website is attempted to be accessed an excessive number of times, far more than the usual expected traffic. This overload on the server will cause some services to stop responding, and eventually, the whole server could crash and become totally inaccessible until it has been physically rebooted. This can be a real pain if the server is not directly accessible to you (i.e. If your server is hosted in the USA)

The operating system can be to blame as a threat to data, a fresh copy of the Windows operating system with no protection (anti virus or firewall) is a sitting duck for malware, as there are many security holes. Also most people who write viruses don't write them to get at Windows users, but rather to get back at Bill Gates (the Chairman of Microsoft)

People also being lazy can have a drastic effect, a lot of system administrators don't change the default password, so many systems across the globe have secure programs with the same password... "password"

The use of public computers can also be a problem. For instance in a library, when a user logs on to sites that contain personal files, some of that information will be stored on that computer (in the form of cookies), it is up to the company who provides the computer to make sure that personal data is not stored on the machine. Most public computers will have very strict security measures in place to prevent people from installing viruses and malware.

## How to prevent

Many sites that make people type in personal data use SSL (Secure Socket Layer), this is a form of encryption that makes sure only the clients machine and the server. The client knows that they have entered a secure site because they will see a padlock sign and the URL would show https:// (notice the “s”)

The system uses public keys to encrypt the data, when it gets to the server, a private key then decodes the data. The SSL site also needs a certificate to prove that the information is being sent to who they say it is.

> *The TLS protocol(s) allow applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint authentication and communications privacy over the Internet using cryptography. Typically, only the server is authenticated (i.e., its identity is ensured) while the client remains unauthenticated; this means that the end user (be that a person, or an application such as a web browser), can be sure with whom they are "talking". The next level of security—in which both ends of the "conversation" are sure with whom they are "talking"—is known as mutual authentication. Mutual authentication requires public key infrastructure (PKI) deployment to clients.* ***- Wikipedia***

A secure way to send money over the internet is PayPal. PayPal, is an eBay owned company that was set up to allow safe money sending over the internet.
Paypal means there is less chance of identity theft, and keeps your data safe. People who sell things on their website, would put a link to PayPal so that the payment could be made on the trusted site. Once the payment has been made thought PayPal, the customer receives as confirmation email.

A lot of companies use PayPal as their online payment system, this is because they don't need to hire people to to manage all the money going into the company from purchases.

PayPal is free to set up, and is free to cancel, this means that more people should be attracted to it as a form of payment.

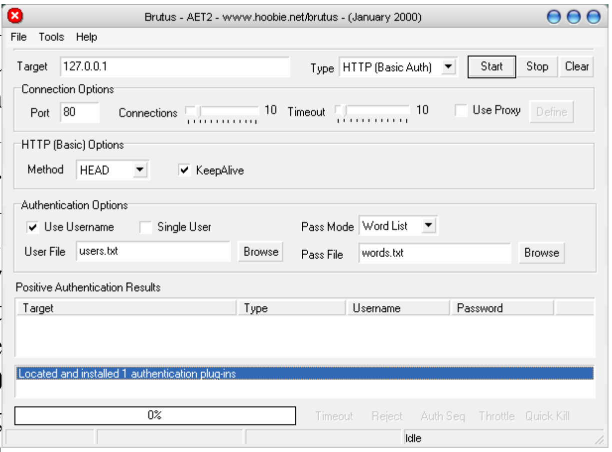
Virus protection is a good idea to prevent a threat to data, a virus checker should be bought, and updated regularly, maybe once a week or more. Also, prevention is better than a cure, so, system Administrators should also, not permit people to run programs, that have not been verified. There should also be a proxy that blocks access to dubious websites.

Another problem is that people may not put their data in correctly. A way that people can make sure their data is not incorrect is to have a verification system in place, this is usually just a second box to type in the same data again.

Where a server is stored is essential when it contains personal data. If someone was to gain access to the server the company's reputation would destroyed. The most efficient way to protect servers like this, is to lock them in a room. Also any backups of the server's data should ideally be locked away too. These backups should be stored in a separate place, so that if there is a fire or any other disaster, then the data is still safe.

Access levels to the server(s) must have limited user accounts so that only few people have full access, this means if anything bad happens, the suspects can be rounded down to a few people.

Strong passwords are the key to a strong system, they should be as long as possible and contain unusual characters (eg @ . , $ & % ! etc.) as well as capital letters and numbers. The password should NOT be a word in the dictionary, as people can generate a list of words to be used in an automated process to try and gain access. If an alphanumeric password is used, then although a brute forcing program (I.e. Brutus AET2) that can go though every single possible combination until the right password is found. Though this can take along time (Brutus can report over 10,000 Millennia) usually the brute forcing program can attempt many simultaneous attacks at the same time, but usually the victim's server will cease to function and could possibly crash.


Brutus - AET2 - www.hoobie.net/brutus - (January 2000)

Target 127.0.0.1
Type HTTP (Basic Auth)

Connection Options
Port 80
Connections 10
Timeout 10
☐ Use Proxy

HTTP (Basic) Options
Method HEAD
☑ KeepAlive

Authentication Options
☑ Use Username
☐ Single User
Pass Mode Word List
User File users.txt
Pass File words.txt

Positive Authentication Results

| Target | Type | Username | Password |
|---|---|---|---|

Located and installed 1 authentication plug-ins

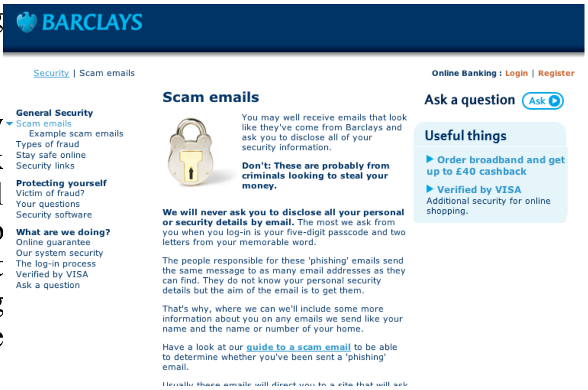
0%

Idle

Illustration 10: Brutus - AET2 by hoobie.net - A famous brute forcing program

Systems should be tested to make sure that they are secure and are unable to leak personal data to the world. Servers should have tight security policies to stop unauthenticated access, which should keep data safe.

Big companies also put adverts warning people about phishing attacks:


BARCLAYS

Security | Scam emails

Online Banking : Login | Register

General Security
Scam emails
Example scam emails
Types of fraud
Stay safe online
Security links

Protecting yourself
Victim of fraud?
Your questions
Security software

What are we doing?
Online guarantee
Our system security
The log-in process
Verified by VISA
Ask a question

Scam emails

You may well receive emails that look like they've come from Barclays and ask you to disclose all of your security information.

**Don't: These are probably from criminals looking to steal your money.**

**We will never ask you to disclose all your personal or security details by email.** The most we ask from you when you log-in is your five-digit passcode and two letters from your memorable word.

The people responsible for these 'phishing' emails send the same message to as many email addresses as they can find. They do not know your personal security details but the aim of the email is to get them.

That's why, where we can we'll include some more information about you on any emails we send like your name and the name or number of your home.

Have a look at our guide to a scam email to be able to determine whether you've been sent a 'phishing' email.

Usually these emails will direct you to a site that will ask

Ask a question
Ask

Useful things

▶ Order broadband and get up to £40 cashback

▶ Verified by VISA
Additional security for online shopping.

Illustration 11: A warning from Barclays

There is a lot of publicity about identity theft, people are advised to check carefully when sending personal information over the internet. Also shredding or burning important documents is also good for enhancing security. Bank statements should be checked for suspicious activities.

Keeping your system updated it imperative if you want your computer free from known bugs.

Some companies will block inactive accounts as they could leak sensitive data, an example of this is MSN's Hotmail service (now known as Windows Live Hotmail) will suspend an account if it has not been accessed once every 30 days.

Wifi connections can be problematic, especially if they are insecure, the best thing that you can do is set encryption on the network, this should be WPA, but if any computers can't handle a WPA connection then a WEP connection (which is less secure) would have to be used.

---

There have been a few acts passed over the years to try and combat internet crime and keep the customer safe:

The data protection act (1984 and 1998)

When you send personal information to a company, they **must** have your permission to pass on the data to other companies, it is usually in the form of a tick box or written in some license agreement.

If data is passed on to 3rd party companies, then the user could be a victim of SPAM, Phone calls and Junk post.

The data protection act states that when a company gets hold of data, they must register and state what they will do with it.

The main principles include the following:

- Personal data should be processed fairly and lawfully.
- Personal data should be held only for one or more specified and lawful purposes.
- Personal data should not be disclosed in any way that is incompatible to the specified and lawful purpose
- Personal data held should be adequate and relevant, not excessive to the purpose or purposes
- Personal data kept should be accurate and up to date
- Personal data should not be retained for any longer than necessary
- Individuals should be informed about personal data stored, and should be entitled to have access to it, and if appropriate to have such data corrected or erased.
- Security measures should ensure that no unauthorised access to, alterations, disclosure or destruction of personal data is permitted, and protection should be provided against accidental loss or destruction.

The act also says that the data can be used by the person's agent, a lawyer, or account for example. Also the data can be used by the people who collected it in the first place. Another exception is if someone's life is in danger and the only way injury or death can be prevented is to release that information. The prevention of crime, tax and duty are also acceptable.

The problem is that the Act relies on people collecting the data, and there need to be more checks to make sure that the law is being taken seriously.

Computer misuse act 1990

This act was passed to address the ever increasing amount of hackers, or unauthorised people accessing system to cause damage.

November 16th 1995 saw the first person in the UK to be convicted under the Computer Misuse act for creating 2 viruses the most famous being "Pathogen"

*In April 1994, the Pathogen computer virus was released in the United Kingdom, by uploading an infected file to a computer bulletin board, where victims could download a copy of the file.The Pathogen virus counted the number of executable (e.g., *.EXE and *.COM) files that it infected.*

*When the virus had infected 32 files, and an infected file was executed between 17:00 and 18:00 on a Monday:*

- *the keyboard is disabled*
- *data in the first 256 cylinders of the hard disk drive are corrupted*
- *displays a message on the CRT that includes: "I'll be back for breakfast..... Unfortunately some of your data won't!!!!!"*

*The Pathogen virus contained a second virus, Smeg, which hid Pathogen from anti-virus software.What makes the Pathogen virus worth including here is that its author is one of the very few authors of malicious computer programs who were arrested and convicted.*

The act includes:

Offences:

- Unauthorised access: an attempt by a hacker to gainunauthorised access to a computer system
- Unauthorised access with the intention of committing anotheroffence: on gaining access a hacker proceeds with the intentof committing a further crime.
- Unauthorised modification of data or programs: introducingviruses to a computer system. Guilt is accessed by the levelof intent to cause disruption, or to impair the processes of acomputer system.

Penalties:

- Unauthorised access: imprisonment for up to six monthsand/or a fine of up to £2,000
- Unauthorised access with the intention of committing anotheroffence: imprisonment for up to five years and/or an unlimitedfine
- Unauthorised modification: imprisonment of up to five yearsand/or an unlimited fine.

Problem is that people are not discouraged from making viruses as the chances of being caught is very slim

The Consumer Protection (Distance Selling) (Amendment) Regulations 2005

This has been set up so that home customers don't have to worry about the laws in other countries when importing from international sites. These are the regulations:

If you buy goods or services over the internet, by mail order or catalogue,digital television, phone or fax, you are protected by the ConsumerProtection (Distance Selling) Regulations 2000, which say that:

- You have a cooling-off period of seven working days after agreeingto the purchase during which you can cancel the agreement.
- The seller must give you clear prior information about the goods orservices, including:
  - A clear description of the goods or services
  - The supplier's contact details
  - Details of cost and payment, including taxes
  - Delivery arrangements, or date for service to be carried out
  - Cancellation rights

This does not apply to:

- One business to another via a contract
- Items bought in an auction with an auctioneer

The Sale of Goods Act

If you buy goods from a trader, The Sale of Goods Act says they must be:

- of satisfactory quality - which means the product you buy should be reasonably reliable.
- fit for purpose - which means it should perform the function you bought it to do.
- as described - means it should be exactly what the trader told you it was.

This act means that if something is not to your satisfaction, it can be returned quickly for a refund, repair or replacement.

In the digital age, we can see that there are many factors that can be a risk to data, these factors can be either an annoyance, or catastrophic! Although the laws are in place, it can be difficult to enforce them. Many of the holes in the systems are exploited by accident so it is unknown when the next attack on your data could be.

Everyone in the top 100 companies in the FTSE index has been targeted by this crime in some way or another. If more people are being caught an punished, then the crime rate should decrease.

The top things that should be done to prevent yourself becoming a victim is to be SAFE:

**S**pyware protection
**A**nti Virus

**F**irewall
**E**nsure your system is updated