Prank the pranksters! Playing around with information and fakes in the age of immaterial capitalism

Fake releases, fake websites, hoaxes: all these tools can be harmful for the power nowadays, let's learn how to use them

Three sections:

- Theoretical analysis
- Some inspiring actions that took place in the past
- Some practical ideas for sending a fake press release/communication

In this text we will discuss about:

- Obstacles for contemporary social struggles, how they connect with the “immaterial” dimension of capitalism
- Communication and hacking techniques: experiments to overcome repression and introduce new tools for social struggles.
- Why these tactics can be useful in our struggles against contemporary capitalism.
- Some inspiring stories of hoaxes that worked well
- Proposals for basic experiments.
- Ideas on how to build your own fake

Theoretical analysis (if you are able to not fall asleep)

Introduction: which context made us think to "prankster tactics"

This text was written as a result of the reflections of some individuals, inspired by collective discussion and processes, about the transformation of society and power. We want it to be a contribution to the experiments that we just mentioned. It deals with certain strategies targeting the immaterial dimension of capitalism, and thus the informational aspect of power. This does not want to be a coherent and ideological work, but a collection of reflections presented pell-mell. This is because we consider that the tactics and ideas we present may be useful instruments for different kind of social struggles. We do not criticize the traditional means of resistance, but we think that many useful tools are sometimes slowing transforming in rooted, never questioned traditions , seen as "safe and politically correct", that at the end tend to repress innovative tools and strategies. We just want to give a small contribution to the debate about new ways of action. In this text you will find some ideas about some new tactics that we want to discuss, followed by practical tips and ideas.

History shows the inventive ways people have found to resist, are practical answers to issues that appear in struggles and every day life...In this present moment, in our opinion, **we consider it vital to evolve our tools of struggle and to experiment several different mediums and ways of action** to overcome the "impasse" affecting social movements. If not, the shortcomings that we do not resolve can come back and haunt us. Capitalism never rests. It always "learns" from our strong and weak points.

Many reason make us believe it is very important to experiment various new ways of action. We will discuss two of them:

- For people involved in social struggles and movements, it is a fact - and sometimes a rather bitter one - that as movements grow, repression gets harder and harder to bear. Experimenting new tactics let us temporarily displace and bypass repression.

- The new organization of work and production make some traditional strategies of struggle less effective. The new industrial organization has grown more and more decentralised, flexible and outsourcing-based. The hierarchical structure of companies and institutions is shifting from internalization to outsourcing, based on subcontracting, indirect control, flexible systems of production and precarious jobs. In this framework, several tactics used in the past seem to be sometimes less effective. Let's take the example of strike. If a company is able to deal with the halt of production by quickly recurring to a subcontractor or a temporary agency, it is less affected. Also, it is much more difficult and less clear to organize a strike in a reticular structure with asymmetric and flexible labour relations more than in the classical fordist large company. **Some similar reflections can be made about the post-fordist transformation of institutions.**

What are the "prankster tactics"?

In the last years many actions involving communication guerilla, hacking, the creation of fakes took place. Some of these practices have been already widely experimented, while others possible paths have, in our opinion, a very interesting potential just marginally explored so far. What we are interested in this text is a form of **direct action aimed at diffusing false information or creating confusion, in order to cause economical or political damage**. This relates to communication guerilla and hacking activism, but it involves some peculiar features that is worth to explore.
We think that a mix of some basic informatics tools, a mimic of the enemy's communication strategies and some information gathering, can produce very interesting and effective tactics, that are often easy to experiment with.

Many actions have already taken place diffusing fake press releases, but they usually had as their main goal the creation of awareness over an issue, denouncing the policy of a specific company/institution, detouring the dominant discourse and unmasking the daily inconvenient truths (even though some of them had without doubts tangible economic impact). Other actions involved cracking, blocking servers, defacing websites, etc., causing serious damage. What activists rarely tried to achieve, however, is causing a negative economic impact by spreading fake information. And doing this may require really simple informatics tools, a meticulous study of the "target", some knowledge of the sector and, sometimes, the help of an "insider" willing to pass some information, tips, etc.

We consider the prankster tactics interesting for several reasons:

- Information is profit

Information is profit. Or to say it differently, an increasing amount of profit is based on information. In the current phase of capitalism, the cognitive dimension is increasingly important. The immaterial dimension of production is taking a central role in the process of valorisation. At the same time every aspect of life is increasingly becoming commodified. Social relations, values or imaginaries, knowledge have become very valuable sources of profit. The image of a firm with customers, retailers, shareholders, and its capacity of generating immaterial value are often more important than the efficiency in physical production of goods. Information is an important resource for companies to control customers, foresee the strategies of other companies and to be able to drawing scenarios for the financial market. Furthermore, the success of a financial institution is based on its capacity to influence the flows of information on financial markets and accessing them in real time.

In the post-fordist economy, the creation of flexible marketing strategies targeted to every single consumer is a central aspect of profitability, and this is the reason why the constant control and the traceability of the individual behaviours of everyone are so valuable. For instance, Google is collecting its huge profits by spying on the Internet users habits, selling them and providing targeted advertisements. As the complexity of the world economic system and the uncertainty are increasing, access to information in order to make a good forecast of the future, has an immense economic value. Especially in financial markets, -where the valorisation process is based on the expectations of the financial actors and strategies are based on a behavioural rationality-, information gathering and rapid scenario play a crucial role. The expectations regarding a company and the courses of its shares, its reputation and the information circulating about the company are heavily influencing the attitude of the market towards the shares and therefore the plus valences related to financial valorisation.

As profit is becoming more and more dependent on immaterial production, **the tactics aimed to hit the immaterial aspect of profit will become increasingly more powerful**. If a company spends millions building their reputation, building up a good marketing strategy and a good information management system, that is a sensible point to hit. Furthermore, this kind of actions may lead firms or institutions to rearrange their operative procedure/communication system/working environment, leading to higher costs. Even physical sabotages or attacks against property, are often producing more indirect damage (loss of reputation, the need to rearrange working procedures) than direct damage (often company goods are insured, and anyway property damage is often negligible compared to the large turnover of a company). In a post-fordist capitalist system, post-fordist tactics of struggle might give us some new ways to fight back effectively.

- Capitalism exploit our brain but also provide us with new weapons for counter attacking

Capitalism exploits our brain - our rationality, our social skills and emotions – and our whole life- as a source for profit. It exploits our cognitive functions, not just during work-time, but also during all of our life span. Our daily behaviour, our imagination, our intellectual creations, become easily - directly or indirectly - appropriated. As they use our brains in their immaterial production, we often acquire several pieces of information and skills (eg. people who work in a company at the same time know the policy and the language of a company and possess the skills to use its technology and systems). **Why not share this information and the skills to counter attack?**

- Make possible to conspire without self-exposing

Furthermore, some people find it difficult to be openly involved in social struggles. Many don't feel like taking part in a social struggle or exposing themselves, but have relevant information and can be keen in smuggling them out. In a precarious and isolated condition (in a broad sense), not everyone wants to start alone an open struggle. But the struggle can also be in sharing information we have and using it to conspire against the companies. Loyalty is a growing strategy of corporate and institutional power in controlling people, and refusing it can be a form of resistance.

-It reverts the relation between mainstream media and radical movements

Finally, the radical social movements often faces a dilemma: how to deal with the mainstream media? Refusing to communicate with them – as they are completely embedded in the capitalism - involves a risk of having our message deformed or our action less visible. Communicating with them, involve the risk of being manipulated and the message deformed. **What about striking back and trying to invert the relation between radical movements and press, trying to turn their constant disinformation on them?** What about trying for once to use media as a vector for spreading fake information? Media are rewriting the reality every day, they are submitted to the political and economical powers and have an almost religious reliance on big press agencies. Many journalists let themselves to believe and reproduce all the information they get from certain sources. Why not take advantage of this weakness for a subversive use, and use the media without being manipulated for once? Why not playing around with media and intervene in their all day and all night propaganda?

Some ideas for possible actions:

- Fake news to publish in the media in order to affect the reputation of a company and disrupt its communication strategy
- A fake mail from a boss, a public servant, etc. can create conflicts or make evident some usually hidden behaviour. It can be an instrument of retaliation.
- A fake press release from a company reporting some fake financial facts in order to affect the stock market.
- Etc, etc, etc!

These examples might serve for different kind of campaigns, social struggles, daily problems...

They exploit our brain - our rationality, our social skills and our emotionality -and our life as an instrument of profit. They mess on a daily basis with our life through financial markets, media spreading irrational fears and rotten ideals, kafkian bureaucracy. Why not counter act at that level and mess up with their beautiful models and their wonderful procedures?

Some instructive stories

Yes Man against Dow Chemical

Dow bought Union Carbide in 2001, and with it the legacy of the Bhopal catastrophe. Dow claims the company inherited no liabilities for the Bhopal disaster, but the victims aren't buying it, and have continued to fight Dow to have an economic compensation. That's a heavy cross to bear for a multinational company; perhaps it's no wonder Dow can't quite face the truth. The Yes Men decided, in November 2002, to help them do so by explaining exactly why Dow can't do anything for the Bhopalis: they aren't shareholders. To do so, the Yes Man created a fake website imitating the Dow Chemical style, DowEthics.com.

Two years later, in late November 2004, an invitation arrived to the 2002 website, neglected since. BBC World Television wanted a Dow representative to discuss the company's position on the 1984 Bhopal tragedy in the year of its 20th anniversary. So a "Dow representative" "Jude Finisterra" (a Yes Man playing this role) went on BBC World TV to announce that the company was finally going to compensate the victims and clean up the mess in Bhopal. The story shot around the world, much to the chagrin of Dow, who briefly disavowed any responsibility as per policy. The Yes Men again helped Dow be clearer about their feelings.

Dow took two hours to notice xhqt was going on; the full interview therefore ran twice, and for two hours the story was the top item on news.google.com. CNN reported a Dow stock loss of 2 billion dollars on the German exchange. After Dow noted emphatically that it was not in fact going to do right by those non-shareholders in Bhopal, the retraction remained the top Google story for the rest of the day.

After two hours, Dow expressed itself more fully by mailing out a more formal retraction: "Dow will NOT commit ANY funds to compensate and treat 120,000 Bhopal residents who require lifelong care.... Dow will NOT clean up the Bhopal plant site.... Dow's sole and unique responsibility is to its shareholders, and Dow CANNOT do anything that goes against its bottom line unless forced to by law." For a while, this became the top story on news.google.com.

http://theyesmen.org/hijinks/bbcbhopal

Whitehaven Coal Hoax

On the 7th January 2013, a fake press release forced Whitehaven Coal into a trading halt after $314 million was wiped off the company's value.

The fake release, produced by activist group Font Line Action on Coal, purported to be from ANZ and claimed the bank had withdrawn a recent $1.2 billion loan to help develop the Maules Creek project. The hoax prompted a sharp sell off on Whitehaven stock, with shares down almost 9 per cent to $3.21 shortly after midday. As news of the hoax circulated the stock slowly gained ground and reached $3.32, down from $3.52, before trading was halted.

The fake release suggested ANZ had withdrawn the loan because of “volatility in the global coal market, expected cost blow-outs and ANZ's corporate responsibility policy.”ANZ policy dictates funds are not to be lent to projects that will have a negative social or environmental impact.“We want our customers to be assured that we will not be investing in coal projects that cause significant dislocation of farmers, unacceptable damage to the environment, or social conflict," the false statement said.

Front Line Action on Coal claimed responsibility for the hoax and said the release was made in order to protest the development of the Maules Creek Coal project.

http://www.miningaustralia.com.au/news/fake-press-release-wipes-$314-million-off-whitehav.html

No Tav attack Intesa San Paolo

At about 9:30 am ET, emails started dropping into reporters' in-boxes. The messages included the stunning claim that Intesa Sanpaolo (IITOF) CEO Carlo Messina had resigned after manipulating the bank's earnings to the tune of $2 billion. The hoax mail included a link to a website that looked very similar to the bank's, and an email address for the press team at Intesa Sanpaolo -- stampa@intesasanpaolo-group.com -- that was almost identical to the real thing: stampa@intesasanpaolo.com

The hoaxers replied to emails sent to the fake address, signing them off "Matteo Fabiani," the real head of the bank's media relations team. Most news organizations quickly figured out something was wrong, but not before the spoof set off a storm on Twitter.

The hoax also sparked what one Italian journalist described as "eight minutes of madness" on the Milan stock exchange. Shares in Intesa Sanpaolo plunged from about 3.11 euros to 2.99 -- or nearly 4% -- in a matter of moments, before bouncing back quickly to about 3.08, where the stock closed.

The action was claimed later by No Tav, which targeted Intesa as the main bank financing the TAV high-speed railway project between Turin and Lyon.

money.cnn.com/2015/04/24/investing/italian-bank-hoax/

Some practical ideas for sending a fake press release/ communication

This is neither an handbook nor a guide, there is no certain theory on the matter, this is more a brainstorming and a collection of tips...

A BRIEF INSIGHT: HOW COMMUNICATION WORKS

Normally companies/institutions have a list of e-mail contacts (press list) to which they send news/press releases/newsletter. Usually it is quite easy to be added to a newsletter. Often you can do it through an automatic form on their website, otherwise you can email their communication office. Their press releases are nearly always formatted in the same way, they present the same logos and structure, and they are sent from the email address.

Press agencies are distributing news to all the media of their country/region. Whatever comes out from them is perceived as truth from journalists. So if you manage to fool one of them, you will likely manage to fool all the newspapers.

The psychology of journalists is an aspect to think about. They often don't check so much the truth of information if they believe the source. If they receive a release they may check the website which is linked, call the numbers which are reported, contact other actors which are supposed to know something about the news.

GENERAL RECOMMENDATIONS: UNDERSTAND HOW TO PROTECT YOURSELF

Don't hurry...
You should take good security measures for protecting yourself and your investigations.
Surfing on the net is like talking loud on the street: many people are able to listen...
When you connect to a website or you use a search engine, usually the website keep your IP address.
The IP address is the number that identifies your Internet connection and allows tracing you. So it's better to connect from a public wireless which is not linked to you!
And even though you are connected from a public place, you can be traced by your MAC address. The MAC address is a unique code which is associated with your wireless card (i.e. with your laptop). But no worries, you can easily spoof it (Macchanger for Linux is an example of a command you can use)...
Your computer itself keeps many traces of your activity, even though you delete everything you think compromising...

Here are a few good tools to be familiar with:

TOR: Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy. Tor can't solve all anonymity problems, but it helps a lot.

https://www.torproject.org/

DISK ENCRYPTION: technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. You can encrypt your hard disk or a usb disk to render the information unavailable to people who don't know the password. The best is to use LUKS on Linux, otherwise Truecrypt on Windows or Mac.

TAILS: a live operating system, that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your **privacy** and **anonymity**, and helps you to: **use the Internet anonymously** and **circumvent censorship**; all connections to the Internet are forced to go through the Tor network; **leave no trace** on the computer you are using unless you ask it explicitly; **use state-of-the-art cryptographic tools** to encrypt your files, emails and instant messaging.

https://tails.boum.org/

These are just some basic hints, spend time to read and learn how to be truly anonymous on the Internet before acting!

You can find a lot of material and tutorials on the web, for instance a good text is:

http://zinelibrary.info/files/FINAL.pdf

Make a lot of tests before acting!

CREATE FAKE NEWS

Let's assume you want to attack the company called Fancy Rubbish
You have to think how to spread your fake info: by e-mail? By Twitter? Creating a fake website and hoping to be contacted by journalists? Mimics need an accurate analysis. Studying the behaviour of your enemy and its communication style is vital for carrying out a successful action. You can do many things: subscribing to the newsletter of your target, checking all the material it puts on-line, making researches.

If you want to send your fake release by mail, you can adopt two strategies: creating a new e-mail address for the purpose (then you need to register the domain of your address – with a fake name of course!), or forging the actual mail from which the companies send out the release. So if your target sends e-mails alerts using info@fancyrubbish.com, you can register the domain fancy-rubbish.com and send the fake release out of info@fancy-rubbish.com. Or even better you can use Telnet, forging their mail and diffuse your release from the original address info@fancyrubbish.com, or – if you think another e-mail address would be more appealing for journalists – from another one, real or invented (communication@fancyrubbish.com, alerts@fancyrubbish.com, fancyrubbish@fancyrubbish.com)

If your target is not communicating a lot, is likely that not many journalists receive their releases and the ones that do don't remember their format and sender. If your target is an important company/institution and has a proactive communication strategy, is more crucial to be a good copycat of the original.

An easy way to correctly formatting the code of a forged fake release is to save the source code of an original mail release, and edit the code substituting the original text with the fake one written by you. Some knowledge of HTML formatting can be quite useful (if the mail is not only in plain text).

If you want to send a forged mail, you definitely need to learn how to use Telnet. If you created a specific e-mail address, you can send it out from your domain. But check for limitations of the service provider before (number of maximum mail per hour, etc...): for mass mail sending, it may be the case that using Telnet will be anyway the easiest and most efficient solution. We will discuss Telnet later.

About the content of your release: think also about hyper links and telephone numbers in your release. Journalists often try to have more info for their story, and check the target website or call the press officer. A smart idea is to make a fake website of your target and to put the link on your release: some journalists will check the site and will be more likely convinced of the authenticity of the story!
About telephone numbers: it is good to avoid journalist to call the correct target numbers, as the target will deny the hoax. Better putting a phone number that a mate will answer pretending to be the spokesperson of Fancy Rubbish. Or to put a number which is occupied or never answering on the day and the hour you plan to act. But make your test before: a voice mail saying to let a message to the post office of Birmingham will make them aware is all fake!

MAKE A SCENARIO

We would recommend you make a scenario, think about when and how to act according to your purposes and how the people will read your news will react.

So you have to ask yourself some questions: your recipients are newspapers or news agencies? Or rather specific people or a specific public? You wish to have your news published as quick as possible on the net? Or you rather prefer to slip it through the day without it being noticed too much and being published on the next day on printed newspapers?

The answers will help you decide the timing. Consider you need some time before your message is read and then published/retransmitted. And the larger is your press list the most likely someone will react quickly. The sooner the fake info become public, the sooner your target will be aware of the fake, and after a short time it will likely publicly deny it.
If you send your release too early, the official denial may come out to early for your plans. If you want to have your release written on the next day newspapers, sending it late enough is a good idea, in order to avoid a denial arriving before the closing hours for newspaper offices. If you want to influence the financial trade the same day, send it out at least one hour before the closing hour of the stock market where the company shares are traded.

TRADE OFF BETWEEN REALISM, INTEREST AND POTENTIAL DAMAGE.

In creating your fake news you should take into account these three axes and achieve a good balance in the final concept.

If you a create way too exaggerate and grotesque fake news journalists will probably have some doubts and double check before relaying the information (even though you never know: it's already happened that media published completely grotesque hoaxes).

If your fake news is realistic but does not represent anything “saucy” for the media, it is too irrelevant, journalist may believe it but not publish it because it is not interesting enough.

And even if your fake news is published, it may not produce the expected harming impact if it does not contain information suggesting a serious threat to the economical solidity or image of the target and that can rapidly spread.

You should create realistic news, at the same time sensational enough for being published and to cause damage to your target. You can get inspiration from the tons of news and releases you can find on the net. And don't be too shy: even if a fake piece of news it is a bit exaggerated and sensational, journalists are not so meticulous and are easy to fool! If in doubt, better exaggerating a bit: it makes more sense to risk with too much sensational news that may cause doubt in journalists and not be published by most of them and it is better to risk a quick deny from the original company, than spread too negligible news that nobody will publish. And if just a couple of journalists will believe the news and quickly publish them, that is already enough!

CHOOSE YOUR PRESS LIST

A realistic fake communication should be received by people that are supposed to receive it. They should receive it in such a way they'll believe it is real. The best option would be to access the actual press list of your target, but that is difficult. Anyway, journalists receive many press releases per day from different sources, they will not be surprised by a release just because it is from an unusual source.

Think also about your public, and how they will diffuse the news. If your press list is composed by newspapers, websites and agencies, they will work as a second level relay, spreading the news exponentially. If just two or three of them believe and publish your hoax, it will diffuse quickly to a large public. So you don't need such a huge press list (but well chosen-some hundreds contacts for country may be enough). If you want to send the news to a final recipient instead (for instant if you pretend to be media), then you can count on a very less relevant relay, so your list should be much larger.

To build up a good press list is not easy, we give you some hints:

- Ask someone that might access directly or through a colleague to the press list of the organization for which she works! Many companies, institutions, association do communicate with media and have a press office which may have a good list of contacts.

- Surf on the net! Many journalists, bloggers, magazines provide their contacts on their site.

- There are several commercial websites selling press lists, you can ask a demo!

- You can extract contacts from the social networks, and with a bit of creativity you can find the email addresses associated to these accounts.

-You can use harvesting bots for collecting all e-mail addresses present on certain websites...

CREATE A FAKE SITE

It can be useful to create a fake website that mimics the original website of the company you want to attack. If you are sending a fake press release by e-mail, it should redirect to the address of your bogus website. For example, if your target's website is located at www.fancyrubbish.com, you could register a domain name with a very similar name, like www.fancyrubish.com or www.fancy-rubbish.com. The easiest thing to do would be to copy the HTML code of the original website and to upload it to your bogus domain. You would only need to edit the HTML code slightly to override the real content of the website with your own bogus content. If the original website contains a list of press releases, you could copy them all and add your own bogus press release to the list. You can easily mirror a whole website with tools such as wget or HTTtrack.
Registering a bogus domain name also allows you to create e-mail addresses that are very similar to your target's official e-mail addresses. If your target sends e-mails using info@fancyrubbish.com, you could create info@fancy-rubbish.com. But this is not entirely needed since the SMTP protocol allows you to send e-mails from a forged address. (cfr. next paragraph)
Once again, be safe and register the domain name anonymously! It is easy to register it with a false name, but more difficult to pay anonymously: Paysafecard, Ukash are good solutions, even though not many domain providers support this payment method.

SEND FORGED MAILS WITH TELNET

Telnet

Thanks to an odd gift of the history of internet, the SMTP protocol (the one used for sending mails) in most cases doesn't require authentication. This means that if you want to send a mail pretending to be info@fancyrubbish.com , you have just to declare that the sender is info@fancyrubbish.com. Really that is all! An extremely easy-to-use program for using SMTP is Telnet: you can send a fake mail in 10 seconds typing few words! We include a short tutorial here in this text, you can find more extended ones on the net.
But remember: **forging mail is not anonymous!** The mails you send will show your IP address... so choose a good open wireless that cannot be associated with you.

Below a box that briefly explains how to use Telnet

Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection

Sending forged emails with Telnet is very easy. We will be connecting to the remote mail server and using the function of mail daemon running in the remote host to send the fake mails.

First open the terminal (or the command prompt, if you use Windows) and type telnet...you will be welcomed by Telnet.. Now we have to connect the mail daemon of the Internet Service Provider through the specific port and the port should have the SMTP service on. Usually, the SMTP port is 25 but that may differ. I also find the port 26 & 587 used frequently for the SMTP service.

For my example, lets say, my ISP is Plusnet, and its SMTP server relay.plus.net is providing mail service through the port 25.
First I connect to the mail server by issuing following command in telnet client: open relay.plus.net 25

This establishes a remote connection to the port number 25 at relay.plus.net. After a successful connection, I am displayed with the SMTP infos. The first time we try a server, it is a good idea to ask help from the mail daemon. So first issue HELP to see the supported commands.

Then we introduce ourselves to the mail daemon by issuing the "HELO" command followed by an identification (usually the best name to give is just the very same name of the smtp server) and after a successful HELO command (answered by 250) , we input the sender email using 'mail from: xxx@yyy.com'. Then we enter the recipient's address using the 'rcpt to: ppp@gggg.org' command.

Now, we enter our actual data using the DATA command. Within DATA, you can fill all the data relevant for your mail: subject, date, format, and many others followed by the actual content of the message. You should learn how to properly format the e-mail content, otherwise you can edit the original code of a real mail you received. Finally, we end our data by entering .(full stop) at the end. This sends the forged mail through that mail server. If the message is successfully delivered we will receive a confirmation message including 250.

Finding a proper SMTP server for your action

Not all the SMTP servers are appropriate. Every ISP (internet service provider) configures its SMTP server differently and it can be tricky to find out the specific policy of each one. Most policies are there to restrict the amount of spam. So, for example, most SMTP servers will limit the number of recipients, the number of connections over a period of time, etc. The network you are using could even be blacklisted by the SMTP server if it has been used by spammers before. It is a good idea to test this thoroughly beforehand, and to check several connections from different ISPs. **You should test your server to check if it is a relay and lets you send your mail to the desired number of recipients, and if the message is properly delivered**.
But be aware to not abuse the SMTP server for testing it: it you are sending too much spam-like communication over the server, they may be thinking spammer are using their server and adopt more restrictive anti-spam policies...
Learn from spammers!

Making a small script

If your mail has to reach a large press list, better using a short script for automating the use of Telnet.
Expect (Tcl) is an example of a good language, available for Linux, Mac, Windows (but if you really want to be safe and anonymous, better switch to Linux). You can find an example of a script at the end of the text.

Understand how antispam works

One of the biggest risks is that your fake mail ends up in the junk mail folder, or does not even arrive.
This can be caused by several factors.

If you send your mail to small number of recipients.
If your mail reaches the spam folder this means probably that the data field (the code of the mail) is improperly formatted, or that you have badly set the HELO. *Double check the code*.

If you send your mail to large number of recipients
Many commercial e-mail providers have strict criteria which can flag your message as spam if sent to large number of recipients in a short time. That is especially relevant for commercial domains (like Yahoo, Gmail or Hotmail), not much for institutional or corporate domains, which have looser antispam filters. If most of your recipients have corporate addresses (as it is normally the case for journalist), be relaxed: this risk don't really concern you.

You can usually find on the net the antispam policy of every single provider.

Some good recommendations for reducing the risk of being blocked by anti-spam filters are:
- not to use a SMTP servers / IP address which is blacklisted for spam reason
- send each mail one by one / and include the recipient line in the data field (avoid sending by chunks)
- try to avoid receiving error messages from your SMTP server, for example by making too many connections at the same time
-choose a good HELO, usually the best solution is to choose the same name of the SMTP server of the ISP you are connected to.

#Annex for the geeks reading this text: example of an expect script (awful but functioning)

The script will open a Telnet session connecting to the SMTP server, and once that is established it will start sending sequential mails
(it sends a single mail to every recipient: that is the best option not to be annoyed by anti spam)

```
#!/usr/bin/expect -f

#The first argument is a text file with all the recipient e-mail addresses
#The second argument is the SMTP server to which you want to connect, usually the local ISP provider of the network you are using
#The third one is the HELO you give to the server. The more anti-spam friendly solution is to put the very same name of the SMTP server
#The forth one is the sender e-mail
#The fifth one is the first part of the data field, till the “To:” field (this can be empty if the data field start with the recipient mail)
#The sixth one is the second part of the data field, after the “To:” field

set timeout 20
set server [lindex $argv 1]
set myhelo [lindex $argv 2]
set sender [lindex $argv 3]
set recipients [lindex $argv 0]
set data_file1 [lindex $argv 4]
set data_file2 [lindex $argv 5]
set rcpt_id [open $recipients r]
set data1_id [open $data_file r]
set data2_id [open $data_file1 r]
set data1 [read $data1_id]
set data2 [read $data2_id]
spawn Telnet $server 25
expect {
     "220"   {puts "ok"}
     timeout { send "QUIT\n" ; puts "SMTP server not answering"; exit}
}
send "HELO $myhelo\n"
expect {
     "250"   {puts "ok"}
     timeout { send "QUIT\n" ; puts "Not answering to HELO" ; exit}
}
set line [gets $rcpt_id]
while { $line >= 0 } {
   send "MAIL from: $sender\n"
   expect {
     "250"    {puts "ok"}
     timeout { send "QUIT\n" ; puts "Connection lost: connectivity problem or SMTP server? Last recipient:", puts $line; exit}
}
   send "RCPT to: $line\n"
   expect {
     "250"    {puts "ok"}
     timeout { send "QUIT\n" ; puts "Connection lost: connectivity problem or SMTP server? Last recipient:",puts $line; exit}
}
   send "DATA\n"
  expect {
     "354"   {puts "ok"}
     timeout { send "QUIT\n" ; puts "Connection lost: connectivity problem or SMTP server? Last recipient:", puts $line; exit}
}
   send $data1
   send "To: <$line>\n"
   send $data2
   send "\n.\n"
   expect {
     "250"   {puts "E-mail successfully delivered"}
     timeout { send "QUIT\n" ; puts "Connection lost: connectivity problem or SMTP
server? Last recipient:", puts $line; exit}
}
   puts $line
   set line [gets $rcpt_id]
}
send "QUIT\n"
expect "221"
exit
```