
E-SEC BY WAY OF
COMMON SENSE

E-Sec
By Way of Common Sense

An IronMarch publication
December 17, 2016
Version 1

TABLE OF CONTENTS

Introduction

Most all internet security manuals you'll ever find deal with the technical and technological side of E-Sec, and the information on the matter is plentiful, not the least of which is the **National Action** manual that we recommend: Security and Anonymity in the Digital Age - A Nationalist Perspective.

The manual you are reading right now, however, deals with the side of E-Sec that does not require any technical or technological know how, no programs, no proxies or VPNs, etc. Instead, it will be dealing with the *Common Sense* of online communications, which deals with how and what you say online, regardless if you are sitting behind a wall of proxies or not. At the end of the day many people tend to be their own worst enemy and no amount of anonymity is going to protect you if you can't reasonably analyze what you should or shouldn't post and say, before you do so.

As this manual is targeted primarily at **IRONMARCH.ORG** forum users it will be foremost dealing with matters especially pertinent to the forum platform, however one can easily extrapolate a more general E-Sec guide from the lessons learned here, this is all dealing with Common Sense, after all.

The need for this kind of manual became apparent the more we've begun to deal with attention that our forum has been drawing from the Media, Law Enforcement and basic bitch liberal scum who think to *"take us down"*. Experience with certain incidents has made it clear that some people do require an instruction in the basics of online communications when one is engaged in or even vaguely affiliated with our Struggle.

Thus we give you the IM Online Security Manual: *E-Sec by way of Common Sense*.

Personal Information

First and obvious step is to completely separate your use of Social Media in a personal capacity and for the purposes of our Struggle, leading a "*double life*" online. Don't use the same logins, profile names, passwords, emails for both personal and openly Fascist/NS accounts, don't ever use emails that contain your real name for the latter; ideally don't even make emails that contain your real name **in the first place**.

Personal use: It is ideal to minimize how much personal information you put out online, something that the modern generation fails to do routinely as online communication has been a normal and everyday thing for it since childhood, thus it is treated with too great of a carefree attitude. Widespread use of Social Media is inherently based on revealing one's personal information, all the way to some platforms demanding one's real, legal ID.

The absolute best option is to **not** have personal Social Media accounts **at all**, they have no real value unless you buy into the bourgeois values and lifestyle (*the compulsive need to share everything about yourself is a prominent example of how this is manifested in online communications*). You don't actually need Social Media to maintain contact with family and real friends - create a dedicated email for those purposes that you release privately only to your family and select friends.

In some instances it may seem unavoidable or extremely useful in daily tasks or for the sake of your education or job, but there are most often ways around this, ways that existed since before the internet. If you find yourself pressed to absolutely have some form of Social Media then minimize what you put out on it to the bare minimum required of you by your situation - try to get away with as least as possible, for example if a real picture of yourself is required do everything to make it obscure (*make it black and white, wear sunglasses, stand at distance, etc*), do not share information on your interests, likes, dislikes and so on. We **strongly** advise **against** ever handing over any real, legal ID information.

Use such accounts only for the **exact** purpose that forced you

to start them, **do not** expand on them beyond that point by adding people you know to the contacts list of your profile, **do not** use it as your primary profile for using the contents of the platform on which it was created, **do not** use it to express any kind opinion or interests. Apply the same principles to other means of online communication.

Example: you are required to have a student email with your real name - use this email exclusively for the purposes of your education (*to communicate with professors*, *receive assignments*, *share materials with other students*), **never** for communicating with your family and friends, let alone comrades in Struggle. **Do not** use that email to register any form of account on any platform or Social Media, instead create dedicated separate emails for those purposes. Consider utilizing temporary emails for short-term purposes or one-off registrations where you are certain you will not require a functioning email afterwards.

We'd go as far as to say that one should altogether avoid using **Facebook** *in particular* for personal use.

Holding openly Fascist/NS accounts on Social Media: to reiterate, we advise that you hold entirely *separate* sets of logins, profile names, passwords and emails that you'll be using exclusively in the Struggle. We recommend using your Fascist/NS Social Media accounts as your primary accounts for browsing whatever platform you are registered on. Obviously one must likewise never use these accounts in connection with anything that is related to your private life and personal information - **never** use them to contact friends and family, for work or education purposes.

In effect, provided that you followed our recommendations on the use of your Personal accounts, said accounts should be empty husks that only contain a minimal amount of personal information while the rest is retained. Your Fascist/NS accounts act on a different dynamic, where there are **no exceptions** to the rule of withholding private information (*you can at most safely reveal your age*, *country and region*), but you can be more relaxed in expressing your attitudes, interests and, obviously, our common views and values.

To sum up, your *modus operandi* should be to maintain **total separation** between your personal and Fascist/NS accounts. The

private information you make available through personal accounts must be **minimal**, the use of these accounts must be **minimized** to specific tasks and kept separate from all others, for example your dedicated email used **solely** for communicating with family and friends. Your Fascist/NS accounts, beyond their obvious purpose, can act as your primary accounts for the purposes of browsing Social Media content that is of interest to you. So long as you maintain total separation, your personal accounts will lack sufficient information to link them to your Fascist/NS accounts, whereas your Fascist/NS accounts would hold no or insufficient information to link them to your persona.

We will again remind the reader, that the advice above is only dealing with the Common Sense aspect of E-Sec. The System can still track and connect your online activities between different accounts if you do not take steps to protect yourself utilizing the technical and technological aspects of E-Sec. On it's own, the advice above protects you from would-be junior e-detectives and doxers who simply need to follow a breadcrumb trail of your own making to identify you, without the need of any equipment beyond their browser. The System can track you the same way without any need in technical means, that it nevertheless has at its disposal, which is where the technical and technological aspects of E-Sec come into play. Common Sense simply prevents you from making it too easy for our enemies to find you. **Do not** make their job easy for them.

Mind What You Say

It is a good rule to assume that everything you ever post or say online is being monitored, regardless of the level of security you are employing - even if not true, it keeps you on your toes and makes you consider what information you may be revealing, even in private conversations, emails, messages. It is already an established fact that IM has been browsed by police from different countries, as well as the media who even publish select user quotes. So mind what you say.

This does **not** mean that one should censor themselves. You are at liberty to express your views and opinions in any way you choose, however don't feed the enemy any information that may lead to tangible negative consequences for yourself (***do not*** *make things easy for the enemy*). One has to be mindful of their particular circumstances - while in the US one can get away with saying most anything, in other countries like Germany the situation can be starkingly different.

To elaborate: the Supreme Court of the United States of America had reversed the conviction of Clarence Brandenburg, Ohio KKK leader, in the Brandenburg v. Ohio case of 1969, holding that government cannot constitutionally punish **abstract advocacy of force or law violation**, defeating the entire premise of the unlawful "*Criminal Syndicalism*" statute, which among other things prohibited the incitement and advocacy of overthrowing the government of the United States by force and violence - theoretical and abstract discussion of violence as means to an end is protected under the **1st amendment**.

We highly recommend our American comrades to familiarize themselves with this case, the legal precedent it set, as well as its consequences. It is precisely thanks to this ruling that William Luther Pierce could write the **Turner Diaries**, and why James Mason's **SIEGE** is not in violation of the US law, hence why he was free to promote and publish the things that he did. Meanwhile the strikingly different situation in Germany requires no detailed explanations.

Research and be mindful of your respective circumstances, while

also being realistic about how much of an interest you could possibly pose to the System. Many people get away just fine with saying whatever they want until they become real persons of interest, so keep that in mind. The more you may be of interest of to the System and its goons the more real the rule of assuming you are always being listened to becomes. Adjust your behavior accordingly.

A simple way to sum up some of the advice in this segment so far: don't post things you wouldn't be comfortable saying out loud with the police in ear shot.

Depending on the nature of your activism, you should never discuss openly your own, or anyone else's participation in a given activity that is not absolutely 100% within the scope of the laws of your respective countries (*as we have already highlighted*, *what is legal in one country may not be so in another*), seeing how some harmless pranks that deserve no more than a warning and a slap on the wrist may be treated as something more than just that. If you are a member of some group you are simply sharing the activity of a group, without highlighting the participation in that activity of specific individuals. In short: **never** openly discuss plans for pranks, **never** mention the pranksters involved beyond group affiliation, unless your group decides otherwise. At most you can share recommendations for other pranksters based on your own experience, again, only at your group's discretion.

Same principles apply to outside of IM with your Fascist/NS accounts on Social Media, with the added mindfulness one must pay to the rules of the platform you are utilizing, and the reasons for which you may be banned from utilizing that platform.

It should go without saying, that one should avoid revealing any private information, as per the advice we've given in our previous segment, extended to publicly viewable messages.

Don’t Talk to Strangers

The most basic advice you’ve received since childhood still applies. Whenever you gain a new contact, such as a new IM user or some new, supposed Fascist/NS contact online, one must be weary and vet the person to see if they are legit, and not some amateur antifa "*infiltrator*" or whatever else.

Be wary of overly friendly new contacts trying to get into your good graces or trying to get you to open up about something. You can maintain a perfectly reasonable conversation with all the advice we’ve provided thus far, which should annoy a potential rat, as such a conversation would not reveal anything of value to them.

Members of groups and organizations in particular should be mindful of new contacts asking about joining their group. Unless you are an official and designated representative of the group in whatever capacity: **do not** speak on behalf of your group, **do not** elaborate on your own role within the group, **do not** reveal any information on internal group workings and activities, **do not** comment on any recent group activities, **do not** carry on *any* form of lengthy conversation about your group at all. Before you make any meaningful reply beyond initial pleasantries and small talk, inform the relevant members of your group of a person inquiring about the group and share with them the exchanges you’ve had with said person up to that point. Let the members of your group in charge of vetting new candidates decide how to proceed and what your response should be. If your group is well organized and vets people properly then there is nothing to worry about, simply let the relevant people handle it.

Some of this advice likewise applies to dealing with the media who may be fishing for any comment at all from rank and file members of a group, especially on their personal opinion as to the nature of the group and its internal goings on. **Do not feed the media anything**, let the designated group representatives handle it.

It should go without saying, that one should also follow our previous advice and avoid revealing private information in any dealing with the media and un-vetted individuals.

When Offline

When you go offline and into the real world much of these same rules apply depending on the circumstances, though they may be more obvious and tangible because of the reality of your actions.

However one thing many still forget is to watch their mouths. Simply don't talk about your online activities or real life activities planned via online communications when out in the real world, unless you are with people who are, as yourself, directly involved in these matters. In fact, if your group exists in close physical proximity it would be best to isolate your plans to strictly low-tech and untraceable or verbal communications done in private and in confidence, rather than divulged online. A good additional level of security is to figure out a code that can be used by your group for strictly online use, with the keys on how to use that code only shared in a personal conversation. Thus if your group operates in cells across long distances it would benefit the group to have representatives of each cell to meet up and decide on an online communications code.

Conclusions

As you can see the advice provided here is extremely basic, truly common sense stuff, however when coupled with the technical and technological aspects of E-Sec, and mindfully followed at all times, you minimize the chances of exposure through your own actions. This manual is meant to help you protect yourself **from yourself**, from absent-minded mistakes and human error that may negate all your technical and technological defenses.

We've included some common sense advice for E-Sec when dealing with group activities, however there is much more to be said about group security in general that is not the subject of this manual. Group organization and security will be a matter for one of the **IM-RFM** manuals that will be released in the future.

It is our hope that you'll take the advice in this manual to heart and adapt your online behavior accordingly. **Remember:** you alone are foremost responsible for your own security and anonymity online - if you do not release some information somewhere at some point *yourself* then there is *nowhere* else for that information to come from. With Common Sense and the technical and technological E-Sec defenses in place you need only worry if you become a big enough person of interest to the System that they would legitimately use extensive resources to break through your defenses. Until such a point in time you can feel safe, but be always vigilant and on guard, both against our enemies ***and yourself***.