Digital Security for Activists

The Riseup Collective

http://zine.riseup.net

Released under the *Creative Commons Attribution-NonCommercial-ShareAlike* license.
Art/Articles copyright their individual authors.

Some rights reserved.

http://zine.riseup.net

funded, or had a lot of people involved in it, so if we can make something, so can you. And you, and you, and you, and before you know it, maybe things will start to get better.

night run to go fix these computers. We even got into a car wreck at 1 AM on one such jaunt. In those days, Riseup needed tons of work to keep going, and we didn't know if it was worth all the hassle. We were volunteering full-time for the project, and it could seem pretty bleak, especially at 1 AM, sitting inside a totaled car. Slow and steady wins the race! Social change doesn't happen overnight, and we are in it for the long haul.

Eventually, we found a secure, temperature controlled, rat-proof lair for all of our computers. This was around the time when our collective grew bigger and stronger, and more people joined up and brought their smarts and hearts to the project.

We now have legal knowledge, media savvy, and education chops to go along with our battle-tested hacking skills. We provide lots of email and lists, and are always working to make everything way more secure. We practice all kinds of mutual aid with other tech collectives worldwide. We are working on Crabgrass, a social organizing platform built on free software, because we think "myface" sites are pathetically limiting and insecure, and they sell us out short just to make a quick-click buck.

So this is our story, at least one of them, and maybe why it's interesting is because some people had an idea and made something new and useful in the world. Riseup has never been well

Contents

Introduction 2

Is the Cure Worse than the Illness? 5

If the Movement has Nothing to Hide 9

Who's the Terrorist? 11

Bandwagons and Buzzwords 22

You're Evited to use the Master's Tools! 27

Pick a Good Password 31

Your Message is Subject to Review 37

Email is a Postcard 40

Google Searches for Busting Unions 42

Blogging with Split Personalities 45

Resources 52

About Us 55

Introduction

Why security matters

Every email takes a perilous journey. It might travel across twenty networks and be stored on five computers from the time it is composed to the time it is read. At every step of the way, the contents of the email might be monitored, archived, cataloged, and indexed.

However, it is not the contents of our online communications that our adversaries find most interesting: a spying organization is most concerned with whom we communicate. There are many ways in which this kind of mapping of our associations is far worse than old-fashioned eavesdropping. By cataloging our associations, a spying organization has an intimate picture of how our social movements are organized—perhaps a more detailed picture than we have of ourselves.

This is bad. Really bad. The US government (like most governments) has a long track record of doing whatever it can to subvert, imprison, kill, or squash social movements that it sees as a threat (forest defense, black power, native rights, anti-war, civil rights, organized labor, anti-slavery and so on), and now they have

About Us

Riseup.net was born out of the WTO protests in Seattle. Or, the original Riseup people had the moxy and pluck to start Riseup after being inspired during those protests. Or something like that. It's hard to remember the exact time and place that folks turned from talking about creating internet tools for activists to acting on it. If you go to mail.riseup.net, you will see our name cut out from a huge sun puppet that marched all over Seattle in 1999.

Riseup wasn't the first project of its kind, and it won't be the last, and from the very beginning we were talking and learning from other collectives doing similar work. When you are strange, i.e. computer geeks with radical politics, it's important to have friends who understand your geek-speak and your anarcho-heart.

For a couple of years, Riseup was run off of one box in one house, and it made a lot of noise and was 'just as reliable as hotmail' (that's what it said on our website.) We were providing email for a handful of people, and all of them knew someone who knew us.

Then we had a couple of boxes in a couple of friend's basements. This led to many a mid-

How-to Guides

The Surveillence Self-Defense Project. Electronic Frontier Foundation.
`https://ssd.eff.org/`
The Organic Internet. May First Collective. 2007.
`http://mayfirst.org/organicinternet`
Practical Security Advice for Campaigns and Activists. 2007.
`http://activistsecurity.org`
Security for Activists. Political Research Associates.
`http://www.publiceye.org/liberty/`
Security in-a-box: Tools and tactics for your digital security. Tactical Technology Collective. 2009.
`http://security.ngoinabox.org/`
Security, Privacy and Autonomy. Resist Collective.
`http://security.resist.ca/`
Communications Security and Privacy. Riseup Collective.
`https://help.riseup.net/security`

all the tools they need to do this with blinding precision.

We believe that private communication, without eavesdropping, and without mapping of our associations, is necessary for a democratic society. We must defend the right to free speech, but it is just as necessary to defend the right to private speech.

Unfortunately, private communication is impossible if only a few people practice it: they will stand out and this will expose them to increased scrutiny. Therefore, we believe it is important for all of us to incorporate as many security measures into our online lives as possible.

What a gloomy picture!

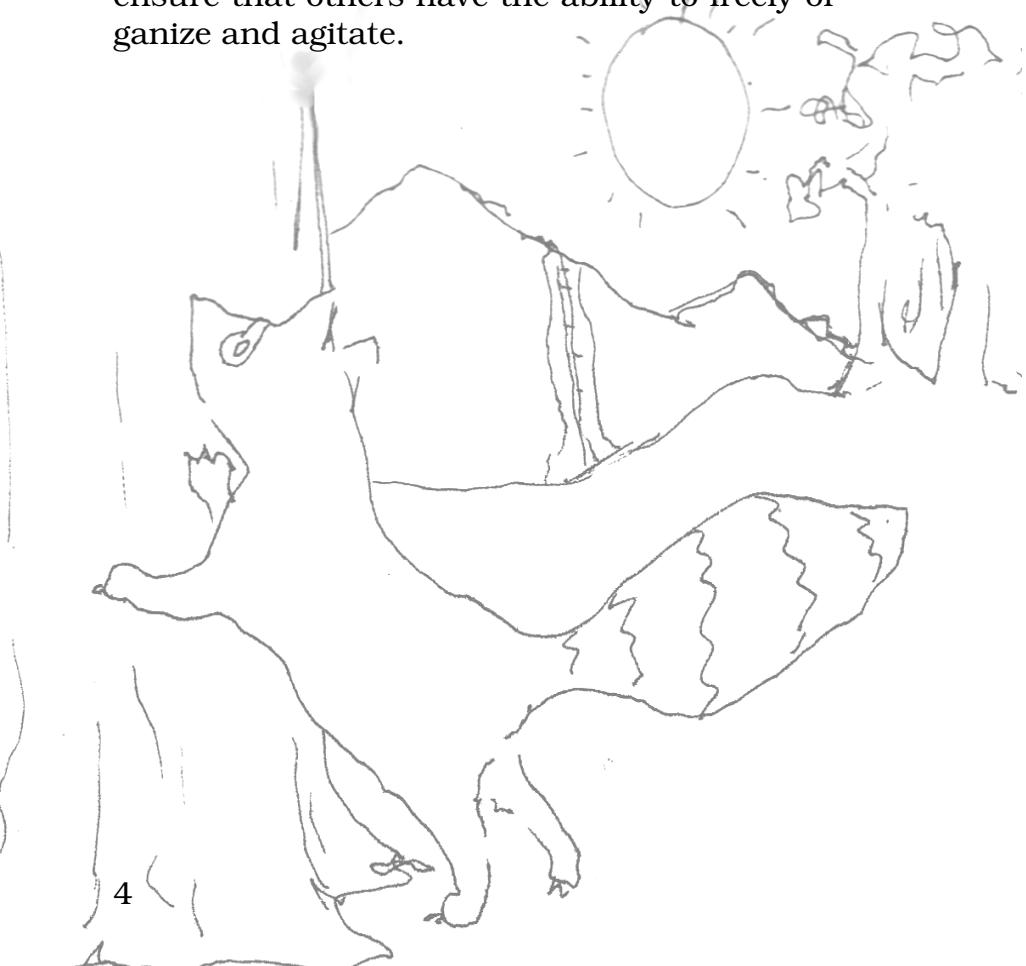
Happily, there are many things you can do. Step one is *education*. Know the risks and know the pitfalls. And make sure your friends and lovers do, too. Step two is *action*. It is not enough to know, we must also do. This zine will help outline some of the simple and not-so-simple things you should know and things you should do.

Do you want a bullet list of priorities for action? Then, here you go:

- *Secure Connections:* by using secure connections, you protect your login information and your data while it is in transport.

- *Secure Providers:* when you send mail to and from secure email providers, you can protect the content of your communication and also the pattern of your associations.
- *Public Key Encryption:* although it requires a little more work, public key encryption is the best way to keep the content of your communications private.

Remember: even if you don't personally need privacy, practicing secure communication will ensure that others have the ability to freely organize and agitate.



2007.
Customer data 'needs protection'. Darren Waters. BBC News. April 21, 2008.
http://news.bbc.co.uk/2/hi/technology/7359263.stm
Printer Tracking: Learn about how your printer might be encoded with identifying information
http://www.eff.org/issues/printers
A compilation of academic essays about various digital culture phenomena:
http://www.ssrc.org/blogs/books/2007/12/31/structures-of-participation-in-digital-culture/

Movies

Big Brother State—An animated short about public surveillance by David Scharf.
http://www.huesforalice.com/bbs/
Privacy and Social Networks. Office of the Privacy Commissioner of Canada.
http://www.youtube.com/watch?v=X7gWEgHeXcA
Taking Liberties Movie.
http://motionographer.com/media/simon_robson/taking_liberties_1.mov
The Spies Who Love You.
http://www.markfiore.com/spies_who_love_you_0
Robots are Taking Over the Web. FreeSpeech TV.
http://freespeech.org/ourweb/
Trusted Computing. benjamin stephan and lutz vogel.
http://www.lafkon.net/tc/

Resources

Interesting Reading

China's All-Seeing Eye: With the help of U.S. defense contractors, China is building the prototype for a high- tech police state. Naomi Klein. Rolling Stone. May 15, 2008.
http://www.commondreams.org/archive/2008/05/15/8970/

Global Gridlock: How the US Military-Industrial Complex Seeks to Contain and Control the Earth and Its Eco-System. Kingsley Dennis, Centre for Research on Globalization. March 31, 2008.
http://www.globalresearch.ca/index.php?context=va&aid=8499

The Nosey Faces Behind Facebook. Rob Argento. Feb. 1, 2008.
http://www.sillyconvalley.net/noseyfaces.html

Border Agents Can Search Laptops Without Cause, Appeals Court Rules. Ryan Singel. Wired News. April 22, 2008.
http://blog.wired.com/27bstroke6/2008/04/

Congress Must Investigate Electronic Searches at U.S. Borders. Electronic Frontier Foundation. May 1, 2008.
http://www.eff.org/press/archives/2008/05/01

Search And Online Advertising: A Continual Evolution. Ellen Siminoff. Search Insider. November 16,

Is the Cure Worse than the Illness?

by PB Floyd

In discussing security culture, activists have to be careful to keep our priorities clear in our minds. Our first priority is action for social change. With that as the priority, it is wise to consider how to reduce risks to ourselves and that is where security culture comes in. But if we focus too much on security culture, reducing risk can easily eclipse the primary priority of taking action to promote social transformation.

I've noticed that a certain kind of paralyzing thinking has increased over the last few years as discussing security culture has become more popular. People and groups get so tied up in making sure their action is secure that they end up not doing the action, or they only do it in a very tiny way with a very tiny group of trusted friends. When security culture makes us too paranoid to publicize any kind of action, our activist priorities have been turned backwards. When we focus too much on security culture, we over-estimate and confuse risks.

For example, there are dramatically different risks in having insecure discussions of an illegal action like a road blockade, lock down, tree sit, or billboard alteration versus having one about arson. All

of these things may be illegal and monitored by the police, but the penalty for arson can be 30 years in prison, whereas the penalties for a lock down are minimal. Sure, it is best that the police don't know that we're going to have a lock down, but if the security measures we adopt make it impossible to organize the action beyond a tiny circle of trusted people, we may have missed the point. Social change requires a lot more than any specific action—it requires building community and a broad social movement. This means moving beyond activist cul-de-sacs, making our process open, accessible, and democratic, and welcoming lots of different kinds of people to join in. Broad openness is directly opposed to a lot of security culture guidelines.

What I've noticed is that security culture tactics that might be very reasonable if one was organizing a highly illegal arson have been popping up in the context of much less risky actions. This weakens our movement. We should not reserve direct action for a tiny group of our trusted friends. The practice and experience of direct action is a life-changing event for many people, and our movement needs *more* places to share these transformative experiences with new folks.

When I was introduced to radical direct action in 1984, I'm pretty sure I never heard a discussion of security culture. It wasn't that we did not realize that the police might be monitoring us with the goal of stopping our actions. Many activists I met then were veterans of the 1960s—they were keenly aware of the FBI's COINTELPRO. But what I remember was that the folks who were my mentors when I was a teenage activist weren't scared or paranoid. They

4. Watch yourself. The key to consistency is to know what your web presence looks like at all times. Subscribe to Google Alerts and Technorati search feeds for all of your names and blog titles to see where they show up on the web. If someone should write about you in a way that violates your privacy, you need to be able to respond right away.

5. Remember that humans make mistakes. Even the most fastidious security geek can relax for a moment and miss a tiny detail that will topple a house of cards and the possibility of mistakes increases exponentially when you start to tell friends what you're doing. Before you write a word on the internet, stop and think about the possibility that your real world identity may someday be connected to it. It's uncomfortable, it's terrifying, and you can work like crazy to make sure it doesn't happen... but just think about that worst case scenario for a moment. Could you survive? Is the risk worth it? Probably? Okay, then get your voice out there!

Five Rules of Persona Management

1. Use separate spaces. If you never ever want your personae to be connected with each other, make sure you're accessing the web from different IP addresses. Public computers at the library are ideal—they're very unlikely to be traced back to you. If privacy isn't critical, on the other hand, try using multiple web browsers (e.g., Firefox for one persona and Safari for another). This will allow you to stay logged into websites that both of your personae use and maintain separate sets of bookmarks.

2. Choose your tools wisely. Are you speaking to a specific group of people or do you want to be seen by the whole Internet? Many social networking websites offer privacy options that can make your persona only visible on a "need to know" basis. If privacy is a concern, limiting your audience may help you sleep better at night.

3. Stick to your boundaries. What are you going to talk about with this persona? What are you going to talk about with that other persona? Are they going to overlap at all? (If so, make sure you don't repeat any content word-for-word under both names.) What rules are you going to set for yourself to maintain your privacy? It's important to honor the commitments you make to yourself, and to think long and hard about it before you change your own rules.

were very aware of the risks and they met the fear with a huge reserve of courage. I remember being at huge, open spokescouncil meetings and huge, open action trainings. It was all very open even though we were pretty sure the cops were watching. And our actions were large and diverse as a result. My first arrest was when I was 16 years old for sitting in front of a train carrying nuclear weapons. Over 100 of us took that bust. The only way to organize actions on that scale (it was part of an on-going campaign of actions) was focusing on openness and not on security.

Discussions of security culture are a more recent trend in the scene and it makes sense in view of 9/11 and the green scare arrests of Jeffrey "Free" Leurs, Daniel McGowen and others. But when we discuss action, we have to keep in mind that few of us will ever take an action like Free took.

I hope that many, even most, of us will have the opportunity to participate in some form of direct action, including illegal actions. Sometimes breaking the law is a necessary part of social change.

Just today, I was faced with this kind of dilemma. I'm involved with a radical community space and we agreed to allow the local low-power pirate radio station to put a transmitter on our roof. Last night, I got the word that it was going up today. The collective that runs the community space has to be an open, non-secure group in order to welcome newcomers and be a publicly accessible portal into the activist scene. So there is a non-secure email list for volunteers—it is very hard to really know who is on that email list because there are new volunteers constantly signing up. Someone had to send

out an email message saying, "The antenna is going up today. If the FCC or the police show up, don't let them in unless they have a warrant." That someone was me—and I have to admit that I felt tense hitting the send button because I knew that sending the email connected me personally with the whole situation. Even if I didn't personally send the email, I and many other people are publicly connected with the space.

Is sending an email like this—or deciding to allow a pirate antenna on your group's roof... risky? Sure it is—it could subject us to fines, police raids, even possibly jail time. There is no way to take this action in a manner consistent with security culture. The FCC can locate the signal from the antenna and it is sitting physically on our roof. We really have to choose to accept the risk and do the action, or avoid the risk and not do the action. So it is a matter of considering the risks, balancing this against the reward, and deciding between fear and fearlessness.

I want us to discuss the security culture, but part of that discussion has to be about when we'll go ahead and do stuff even when there are clear risks that can't be mitigated or avoided. Hopefully, our discussion of security culture will emphasize that if it makes us too paranoid or careful to actually act, then we've lost our way.

Finally, my web identities became too fractured for me to manage and I decided it was time to reconcile it all. I came out on my professional blog as queer, announced myself as the editor of Genderfork, and braced myself for a fall-out of drama and controversy. The results were surprising. I received an endless stream of support and encouragement and my professional relationships strengthened immediately. Within two months, I was interviewed on television and the radio about my grapplings with identity issues, was invited to guest blog on several websites, and was asked to be on a conference panel about "coming out" on the Internet. My blog readership has grown considerably, and I feel protected by a safety net of people who are emotionally invested in encouraging me to be myself. Seventh lesson learned: the general public is much more capable of accepting me than I gave them credit for.

Sarah Dopp is a blogger, poet, and website development consultant in San Francisco. She is also the editor of Genderfork.com, a project that explores androgyny and gender variance through artistic photography. Read more at: `http://www.sarahdopp.com/blog`

sion of content in my life: things that belonged in my locked Livejournal, and things that belonged on my public blog. Since I had different audiences in each space, I started to develop two separate reputations: people either perceived me as professional and clear-headed, or as messy and neurotic. In my less confident moments this affected my self-image, and I began to think of myself as dishonest. Fifth lesson learned: When I'm managing multiple personae, I'm not representing myself as a whole person.

With all these lessons piling up under my belt, I decided to try my hand at something new. I started a blog called Genderfork.com, where I posted daily photos of androgynous people and discussed issues around gender variance. This project was way outside of my comfort zone, so I used a pseudonym and only told my closest friends about it. I was afraid that it wouldn't go well, that people would leave abusive comments, or that it would deter future clients and employers from hiring me. Miraculously (to me), the project was successful. People left encouraging comments, thanked me for creating the site, engaged in the conversation, and recommended photos for me to use. I became proud of the project and wanted to share it with other people, but realized I wasn't set up to do that. Sixth lesson learned: My separate personae do not get to take credit for each others' accomplishments.

StartTLS: If the Movement has Nothing to Hide...

by House Sparrow

In the waning days of Babylon and empire, what will the US government think up next? According to leaks from sources ranging from the intelligence bureaucracy to the New York Times, the New Yorker, and the Wall Street Journal, the government's new fun toy is the ability to monitor our social networks by tracking, in real time, the patterns of email, phone calls, text messages, and financial transactions. This program is top secret, so you can't take legal action because you can't prove the program exists (according to the catch-22 logic of a February 19th US Supreme Court decision).

The Clinton, Bush, and Obama administrations said the program is entirely constitutional because it does not involve eavesdropping on the content of our communications. Instead, it focuses on the pattern of our relationships. In this way, individuals are not under surveillance, all of society is. If your social movement has nothing to hide, then what are you worried about? Plenty. This kind of map of our

social networks creates a ready made blueprint for disrupting any social movement deemed to be a threat. In many ways, the government knows more about how we organize than we do. This issue is important to all organizers, because much of the world's email is routed through the US.

So, what can we do about it? For starters, get everyone you know to start using an email provider that uses StartTLS. For email, it is the only thing that can protect against the surveillance of our social networks. For a list of StartTLS providers besides Riseup see:
`http://help.riseup.net/security/measures`

What about phone calls, internet chat, and social networking sites? Your riseup birds don't have all the answers, but we are working on it. One thing we know, privacy and security are not solved by personal solutions. If we want security, it will take a collective response and a collective commitment to building alternative communication infrastructure.

to decide how to do that.

My next major blog started off public and then later became private. I created it on Livejournal.com, wrote under my real name, and used it to speak freely about my emotions, opinions, and relationships. I was wrestling with gender and sexuality issues and I needed a place to write it all down. I shared it with my friends but didn't mention it to my family or work contacts, and just trusted that it would stay off their radar. A year into the project, I realized I was censoring my own writing out of fear that it would be discovered, and I started to resent the project. Livejournal, fortunately, has excellent privacy settings, so I changed the entire blog over to "friends only" access. The downside was that my journal became harder to read—friends had to log in to their Livejournal accounts in order to view it, and it could no longer be found by the casual web surfer. The upside, though, was that I felt (mostly) free and safe to write without editing myself, and that's an incredible gift. Fourth lesson learned: Sometimes I need to choose between freedom and visibility.

After a few years of living behind a locked Livejournal, I realized I missed having a public voice, so I started another blog. I created it at SarahDopp.com, considered it my professional web presence, and knew it would stick with me for a long time. I was careful to only write things that made me look respectable, reliable, and valuable. This created a clear divi-

listed on an obscure page at the main college website, which you could find if you browsed deep enough into the menus. Prospective freshmen, it turned out, were inclined to browse that deep. Since I was one of the only people at the college making use of my student web space, I started receiving daily emails with questions about the campus from high school seniors all over the country. Second lesson learned: I can give myself a voice, but I can't control what it means to other people.

I spent the following summer in China, living for four months on my own after a brief study abroad session ended. The cultural differences were jarring to me, and I needed a way to tell the stories to my family and friends back home. I started a blog on Blogger.com with a few self-imposed restrictions: I wouldn't tell anyone in China that I was doing it and I wouldn't use my last name or my Chinese name. The arrangement was perfectI could speak freely about my discomforts and misadventures without offending anyone around me, and I could keep my U.S. contacts aware of how I was doing. Unfortunately, my sensitive grandparents also heard about the blog, read some of my more dramatic stories, and became very upset about how dangerous my overseas situation seemed to them. From then on I continued to tell exciting stories, but I made sure to edit my posts to emphasize how safe I was. Third lesson learned: I have a responsibility to respect my audience, but I get

Who's the Terrorist?

Blogging Against Surveillance

by Anne Roth, annalist@riseup.net

On July 31 of 2007, at seven in the morning, armed police stormed into the apartment I share with my partner, Andrej Holm, and our two children. We learned that day that Andrej was a terrorism suspect and that an investigation had been going on for almost a year. Andrej was arrested and flown to Germany's Court of Justice the next day. The search of our apartment lasted fifteen hours. I was forced to wake my children, dress them and make them eat breakfast with an armed policeman watching us. That day my new life started, a life as the partner of one of Germany's top terrorists.

Andrej spent three weeks in investigative detention. The details of how the arrest warrant was issued caused a public outcry, not only in Germany but also in many other countries. Open letters were sent to the court that were signed by several thousand people protesting the arrests. Among the signatures were those of David Harvey, Mike Davis, Saskia Sassen, Richard Sennett and Peter Marcuse.

What had happened?

Hours before Germany's federal police came to our home, three men were arrested near Berlin who were said to have tried to set fire to several army vehicles. The original investigation was started against four other men, of whom Andrej is one, who are suspected of being the authors of texts written by a group called "militante gruppe" (mg, militant group). The group is known in Germany for damaging property for years, but never using violence against people. The texts are claiming responsibility for arson attacks against cars and buildings since 2001. German anti-terror law §129a of the penal code was used to start an anti-terror investigation against the four. All of them write and publish online. Andrej works as a sociologist on issues such as gentrification and the situation of tenants. Outside academia he is actively involved in tenant organizations and movements that deal with gentrification and city development. Since 'militant group' uses words such as 'gentrification', 'marxist-leninist', 'precarisation' or 'reproduction' and Andrej also uses terms like these in his research papers, the state considered this sufficient evidence to justify complete surveillance (a subsequent linguistic analysis by the Federal Police later showed its most unlikely Andrej wrote these texts). As we later learned from Andrej's files, the profile for the 'militant group' was based on several assump-

Blogging with Split Personalities

How I Created and Reconciled My Separate Spaces On the Web

by Sarah Dopp

Hi, my name is Sarah, and I'm a compulsive blogger. It all started in high school when I created a website under a pseudonym and used it to tell stories about my love life. It was a thrilling and introspective project that resulted in a lot of great writing. Unfortunately, I was so terrified someone would connect it to me that I never saved a backup copy. That website has since expired and those words are now lost forever in the murky underbelly of the Internet. First lesson learned: If I'm not going to claim something, I can't hold onto it.

My next blog was more open but less personal. In 2001, my first year of college, I used my student web space to keep an online journal about my day-to-day interests and experiences. I kept each post short and simple and figured no one would care about them except me. I was wrong. A few months into my semester, I discovered that the school's student websites were

ble use of the net, and that the net offers us new possibilities for organizing, campaigning, and strengthening our unions. The low cost and global reach of the net, we believed, would empower unions and level the playing field in the struggle with employers.

But the net also offers new possibilities for union-busters and there is some evidence that corporations are using the net more effectively than we do.

How do we cope with the dangers of data-mining and net-based blacklisting? We need our members and especially our organizers to learn some of the basic skills for protecting their privacy online. We hear all the time about how teenagers are being warned that what they write today on MySpace and Facebook can come back to haunt them when they apply for their first jobs, but where are the unions warning members how to behave online, how to protect their identities, encrypt their correspondence, visit websites anonymously? Which unions are creating for themselves secure areas for online discussion that are not easily data-mined by the opposition?

As the Starbucks example shows, some employers have thought this through and are way ahead of us in the game. We in the trade union movement need to begin training our officers, staff, members and potential members in the art of survival in an age when privacy is increasingly becoming a thing of the past.

tions. Members of the 'militant group' are assumed to: have close ties within the group (all four have been good friends for years); be leftist political activists; have no prior police record; use 'conspiratorial behavior', such as encrypting email and using anonymous mail addresses (not made of proper first and last names); be critical researchers and as such have access to libraries and a variety of daily papers; and have profound political and historical knowledge.

The initial suspicion, which was based on internet research for similarities in writing and vocabulary, led to surveillance of several forms: phone tapping, video cameras pointed at living spaces, emails and internet traffic being monitored, bugging devices in cars, bugging operations on people's conversations, etc. None of these produced valid evidence and so every two or three months surveillance measures were expanded. Anti-terror investigations, according to 129a of the penal code, are known and infamous for the fact that they are being carried out secretly and that less than 5% ever produce enough evidence to lead to actual court cases. The vast majority entail lengthy investigations, during which huge amounts of data (mostly on activists) are collected, and after years of activity the case is dropped without anyone ever knowing about it.

The 'terrorist' deeds themselves are not being prosecuted, but rather membership in or support of the named terrorist organization. There-

fore, investigations focus on 'who knows who and why.' At this moment we know of four such cases carried out against 40 activists in Germany last year. Participation in protests against the G8 played a prominent role, but not the only one. In all four cases the names of more than 2000 people were found in the files that were handed over to the defendants: a good indicator of what these investigations are really good for.

In our case it is likely that all people who had any kind of interaction with Andrej during 2006-7 were checked by the police. As a result, they discovered two meetings that allegedly took place in February and April of 2007 with someone who was later included in the investigation as a fifth suspect, and then two other individuals who were in touch with this 'No. 5'. The two meetings took place under "highly conspiratorial circumstances": no mobile phones were taken along, the meeting had been arranged using so-called anonymous mail accounts, and, during the meeting—a walk outside—the two turned around several times.

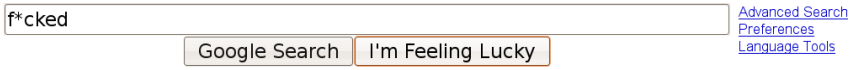
The three who were included in the investigation are the same three who were arrested after the alleged arson attempt. Some hours later special police forces stormed our home and Andrej was dubbed 'the brain behind the militant group.' My identity changed to that of 'the terrorist's partner.'

managers discovered that two pro-union employees in New York were graduates of a Cornell University labor program... Managers took the names of graduates from an online Cornell discussion group and the school's website and cross-checked them with employee lists nationwide. They found that three employees in California, Michigan and Illinois were graduates of the program and recommended that local managers be informed."

That's pretty clever – Starbucks was not only looking for troublemakers, but also for potential troublemakers, or people who might have sat in class next to troublemakers. It was chilling for me to read that they were specifically targeting Cornell labor program graduates. That brought home to me the point that if this technology had existed in 1974, it would not have been possible to covertly insert someone like myself into a non-union factory.

Using the techniques of data-mining, human resources staff will be able to block the employment of not only trade union organizers, but of people who might be friends with union organizers. If I were a union-buster, the first thing I'd do is sign up with Facebook (where one is actually faceless and anonymous) and "friend" all the union activists I could. In the real world, this would be tricky, expensive and time-consuming. But not online.

Many of us, myself included, have long argued that unions should make the best possi-



Google Searches for Busting Unions:

How the Internet makes organizing harder

by Eric Lee, originally published in Industrial Worker

Back in 1974, I was a student in Cornell University's labor relations program working during the summer for a union in New York City. The union's education director (today its president) suggested to me that I quit university and go to work in a factory where I could organize workers. That was the way to get involved in the trade union movement, he told me. I pondered the offer—it would have involved moving to Indiana—and eventually decided not to do it.

Thanks to the Internet, that scenario is no longer possible.

I had been a political activist for a few years by then (I started quite young) but there was really no way for a factory owner in Indiana to know who I was. I probably could have covertly entered the factory and helped unionize it.

Today, factory owners are a mouse-click from knowing everything about each of us. The old strategy of blacklisting—employed so successfully against unions for many years—has now become infinitely more effective thanks to the net. According to a recent report, "Starbucks

What to do?

I was in shock. Berlin was on summer break. The few of us who were not away got together to gather the little we understood about the accusations. The media rejoiced with headlines such as 'Federal Police finally succeed in arresting long-searched-for terror group' and we had to deal with media inquiries, talk to lawyers, talk to relatives, talk to friends, colleagues, neighbors and our children. We had to learn about life in prison, start a campaign for donations to pay for lawyers, create a website, agree on how to proceed with a rather heterogeneous group of suspects and an even more heterogeneous network of friends and supporters, and discuss how to deal with the media.

I slowly realized that my children and I were the collateral damage in this case. My computer was confiscated, items were taken from my desk, all of my belongings searched. My kids (2 and 5 years old last summer) lived through two searches conducted by armed police. Their father was kidnapped and was not returned for weeks.

Being a political activist myself, I am of course aware of the fact that phones can be tapped and that this is used extensively against activists. In Germany close to 40,000 phones (including mobiles) are tapped each year we have a total population of 80 million. To realize and later to read on paper that this concerns you is entirely

different from the somewhat abstract idea that you may be subjected to it.

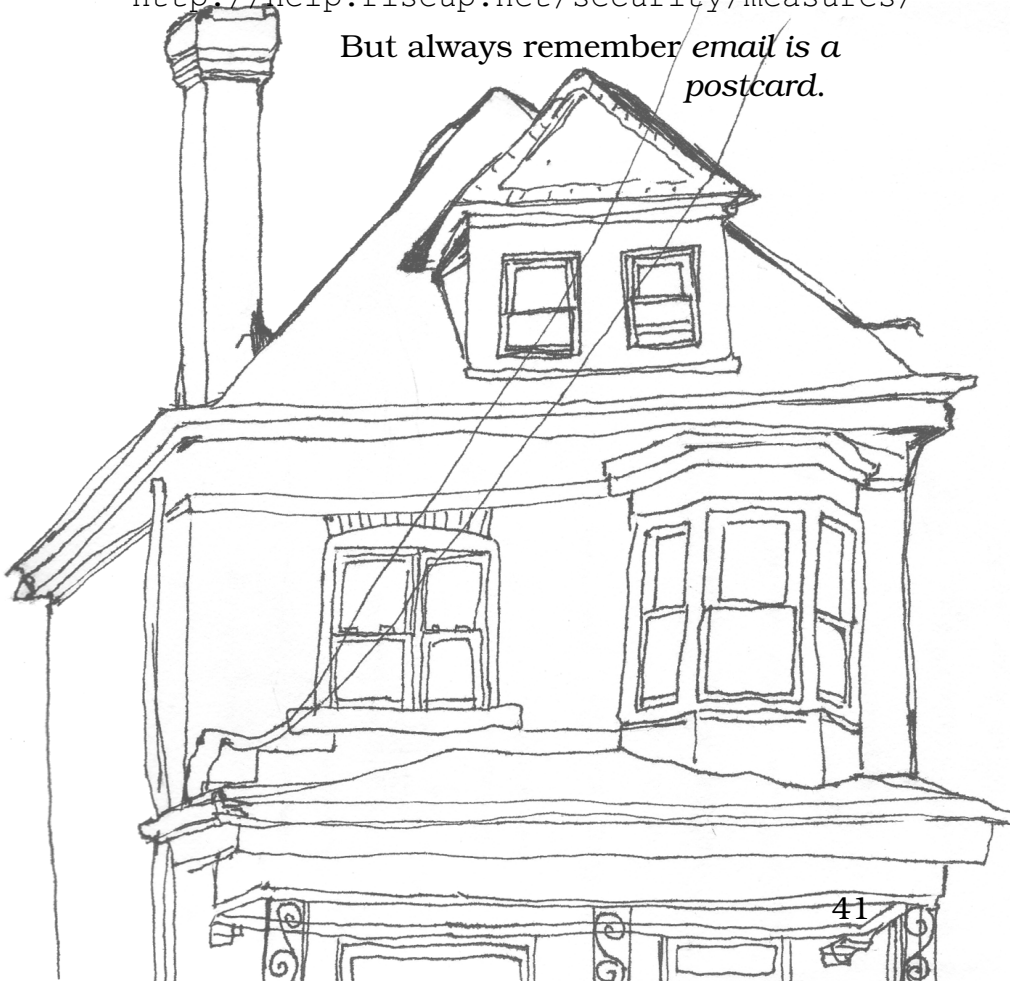
When Andrej was released on bail after three weeks, the Federal Prosecutor of Germany filed a complaint and wanted him back in detention right away, based on the idea that he might flee the country or that there was danger of repetition. How do you repeat membership in a terrorist organization? One of the many mysteries inside the prosecutors mind. The complaint was not granted right away but instead Germany's Court of Justice decided it needed time to reflect thoroughly on the details of the arrest warrant (which was the origin of the huge wave of solidarity that was widely covered in the media), the question of whether the so-called group actually qualified as 'terrorist' and whether the presented evidence justified detention.

It was impossible to miss the fact that Andrej was the focus of police observation. Our phones went crazy—more than once people tried to call Andrej's mobile number but ended up on my phone instead. When I tried to call him, I got my own mailbox talking to me. Our TV behaved funny (as a result of silent or stealth pings that were sent to Andrej's mobile phone regularly to locate him). Emails disappeared.

At some point in the middle of this I considered starting a weblog. To my knowledge nobody had ever written a blog about living under anti-terror surveillance. It was not an easy decision: were people going to believe me? Would

its contents. Maybe most people don't choose to, but you should know that they definitely could. Some places won't. Riseup won't, but we're not the only ones involved. If you were to send detailed information about your affinity group's plans for nonviolent direct action to end war and you were to send it on a postcard that the Department of Defense happened to help carry on its way, don't you think they might want to take a peek? For information on sending e-letters in an envelope, see:
`http://help.riseup.net/security/measures/`

But always remember *email is a postcard.*



Email is a Postcard:

Good security is no substitute for good sense

by Blue-footed Booby

Email is a postcard: email is a word that barely existed 25 years ago. But what is that word? It's "e" for electronic, stuck together with "mail," which, way back when the term was invented, must have referred to the little pieces of paper moved from place to place by postal services. There were lots of different types of letters back then, though. There were the letters in thick legal envelopes that you couldn't see through, good for concealing cash when donating to Riseup or ordering fanzines. There were those flimsily enveloped letters that you could hold up to the light to make out some of the words in a love letter. 8.5 × 11 yellow ones full of unfolded papers, padded ones that kept mix tapes from being crushed. What kind of letter should we imagine when thinking of the anarchist postal worker delivering an email through the internet?

Email is a postcard. Anyone involved in the transmission of your precious email can read

I be portrayed as crazy or paranoid? On the other hand, unlike many other people I knew for sure that surveillance was taking place, so why not write about what it felt like? Germany had a major debate about data retention last summer—the law had just passed and was to go into effect 2008. A new anti-terror federal police law was discussed in parliament and a public debate about data protection grew to dimensions nobody had thought possible some months before. The War on Terror serves to justify more repressive laws here as well. A blog about the consequences of an investigation into a family that is admittedly interested in politics (and actively involved), but otherwise not exactly the typical terrorist stereotype, could open many eyes.

Initially, I did not like the idea of blogging, precisely because I am quite fond of my privacy. Why present my personal daily life to a largely anonymous public? Absurd. But now, after my privacy had been violated beyond imagination, why not talk about what it feels like to people who are more sympathetic than the Federal Prosecutor? Why not talk about how ridiculous the 'facts' to prove the case really are? And there are so many amazingly strange interpretations of how we live our life, of what Andrej said on the phone, of what my mother said on the phone, that I thought nobody would believe these details just some months later.

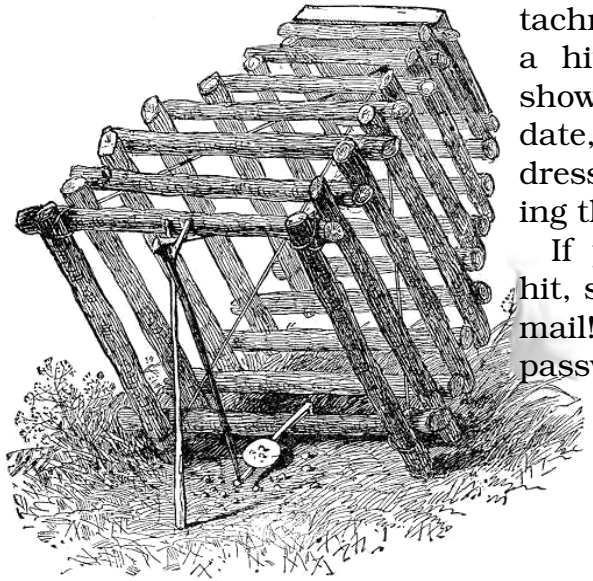
And so I started blogging. Mostly in German,

primarily because I didn't find the time to translate more, but also because I thought that interested readers would mostly be German. You can find some texts in English there, too, however.

I wasn't familiar with the world of blogs, and probably still am not. I didn't have time to find out how to 'make your blog popular' and was not particularly interested in doing so. I wasn't really sure how much attention I'd like. I started by publishing in the blog the same things I had emailed to people interested in the development of the case and in how we were doing personally. I only told people I knew about it. It took about three weeks before some of the more popular political German blogs picked it up and wrote about us, and then the number of visits exploded. In the beginning people wondered whether this, and I, 'was real.' The blog received lots of comments and it was obvious that many people were completely shocked about what was happening. They compared the investigation to what they imagined having taken place in the Soviet Union, China, North Korea, East Germany, but not 'here', in a Western democracy, a constitutional state. Another group consisted of people who wanted to help us secure our privacy. They explained email encryption, switching SIM cards in mobile phones and the like, not realizing that at least in the first months we actively avoided anything that could make it seem like we wanted to behave in a conspir-

counter (such as `onestatfree.com`). Fake the information you provide, if you like. After signing up, you will receive some emails, and one of them will include an attachment with a filename like `OneStatScript.txt`. Write down your OneStat account number and delete the email.

Now, change the name of the text document to something that would entice someone snooping on your email, such as 'passwordlist' or 'myaccounts', change the extension to `.htm` and make sure the format is html. Then, email the file to the email account you would like to monitor. Now test it by opening your email and then opening that attachment. By opening this attachment, it should register a hit with the website hit counter, so login there with your account information and see if a hit was registered. Now just let that enticing email sit in your account and periodically check your hit counter.



If anyone opens this email and finds the attachment and opens it, a hit will be recorded, showing you the time, date, location and IP address of the person opening the attachment.

If you have even one hit, some is reading your mail! It is time for a new password.

tached to it in any manner." Private Art School, your message is loud and clear. The time for a new method of inter-web communication has come.

Maybe it is legal for colleges to screen emails, but it is not something I, or any of my friends, want to be subjected to.

More secure email providers such as Riseup and Hushmail are what I gratefully turned to. Riseup's webpage prominently features something refreshing: "We will not read, search, or process any of your incoming or outgoing mail other than by automatic means to protect you from viruses and spam or when directed to do so by you when troubleshooting."

Of course, it is not just what server you select that makes a difference in how secure your personal message is. Obvious things such as password security and logging out when you finish are things that can easily be overlooked. Public computers, such as the ones at libraries, are used by countless individuals each day. Forgetting to log out will leave your information open to the masses.

Commercial email providers are offering more and more storage space for "free", so people are using their accounts to store anything and everything. Bank account numbers and names, backup documents, along with personal emails are all in the system waiting to be hacked.

Want to secure yourself? Of course you do. One clever trick is to sign up for a website hit

atorial manner, as this was one of the reasons Andrej became a suspect to begin with.

I thought it was pretty funny that because I was 'the sociologist's wife' (we are not married), people seemed to assume that Linux or encryption were things I'd never heard of. Many people expressed fear that by reading my blog or commenting on it they might endanger themselves. I was glad they did anyway. Others expressed admiration for our choice to be so public about the case. All of this was great and very important support that made it much easier to deal with the ongoing stress and tension that comes with the threat of being tried as a terrorist.

Fortunately, the Court of Justice made several decisions that were very favorable for Andrej. First, two months after the prosecutor's complaint about his release on bail, the court decided not only to deny the complaint but also to completely withdraw the arrest warrant, arguing that 'pure assumptions are not sufficient.' This decision was perceived by many journalists as a 'slap in the face' to Germany's Federal Prosecutor . One month later the same court decided against the 'militant group' being considered a 'terrorist organization.'. The German definition for terrorism demands that a terrorist act be intended and able to shake the state to its very foundations, or else to terrify the population as such. Germany's minister of justice, Brigitte Zypries, was asked about the case against the alleged members of the 'mil-

itant group' in an interview with Der Spiegel, one of the biggest political weekly magazines, and she said that she thought that the September 11 attacks were a terrible tragedy, but not a terrorist act by her definition as they didn't manage to endanger the American state. We were rather surprised by this, to say the least. In November the Court of Justice decided that the 'militant group' can't be considered terrorist and ordered that the other three people arrested be released on bail. Now the investigation is being carried out under §129 (instead of §129a), which prosecutes criminal instead of terrorist organizations, with possible sentences up to five, instead of ten, years.

When Andrej was arrested for 'being a terrorist', on the grounds of being intelligent, knowing many people from different spheres of society, accessing libraries, and publishing texts, it felt possible that they'd sentence him to a prison term. But after months of public support and with more details of the investigation becoming public, I, like many others, starting believing that this nightmare was terminal, that the case would have to be dropped eventually. Most people don't realize that the investigation is actually still going on. All of our phone calls are still being listened to, our emails read, Andrej's every step is being watched. Germany discusses online searches of computers and using hidden cameras in people's living spaces to detect terrorists and we know that the secret service is

Your Message Is Subject To Review

by jacqueanne

I opened up an email from Savannah College of Art and Design and my eyes focused on an unexpected phrase: "Your message is subject to review." Wonderful. As a recent transplant to Savannah, I was trying to make contact with certain "dangerous people", such as whoever coordinates the local Food-not-Bombs. Was something in my email asking when I could help feed the homeless suspicious enough to be "subject to review?" Why is SCAD screening my emails to begin with? Perhaps the word "bombs" triggered something in the SCADmail system. Or maybe my educational institution is randomly screening my emails. Either situation is uncalled for: no one is going to write in a casual email, "Hey, I'm bombing the fashion building Thursday at 2pm sharp—just to let you know. Hope all is well."

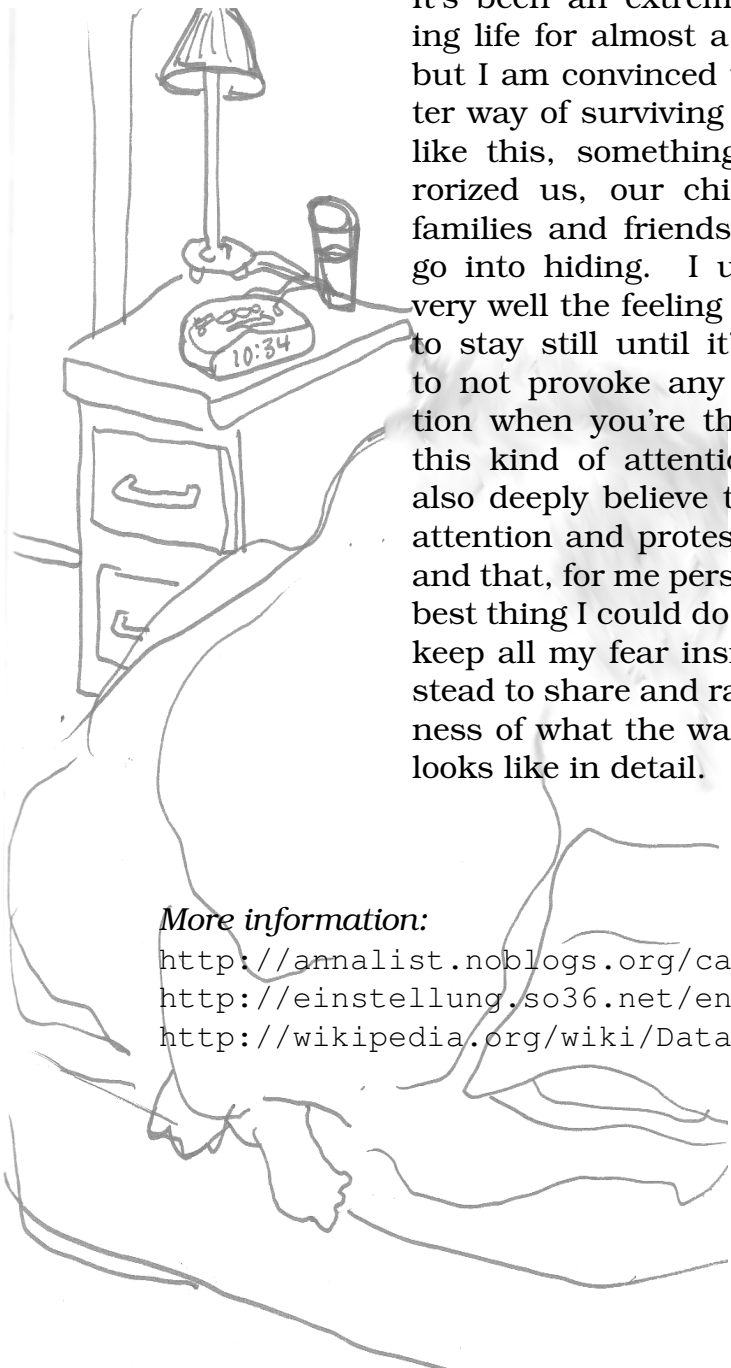
If my email did get reviewed, it must have been denied silently because it was never sent. I think this is SCAD's way of saying, "We do not want to be connected with anything slightly controversial, so we can not allow an email to an activist group to be sent with our name at-

top of those, short of outright robbery and identity theft (which do happen, and would probably be bad) there are a few other sorts of things that might go terribly awry if you aren't being smart about passwords and privacy:

- Someone could gain access to your email account, either because you logged in from a public terminal and didn't log out, or because you logged in using a public wireless connection and someone sniffed out your signal. They might use your email account to send great quantities of spam, which could get your email provider blacklisted or get your account shut down. They might use your email account to send desperate messages to everyone in your address book begging for money (it happens pretty often).
- Someone could use your (S)FTP login or website login to place a malicious script online that logs everyone else's password attempts, and sends home a tidy little list of good username and password combinations to try on email servers.

(cc) LINC Project April 2006
Creative Commons AT-NC-SA 2.5

using what the police only dream of.



It's been an extremely straining life for almost a year now, but I am convinced that a better way of surviving something like this, something that terrorized us, our children, our families and friends, is not to go into hiding. I understand very well the feeling of wanting to stay still until it's all over, to not provoke any (legal) action when you're the focus of this kind of attention. But I also deeply believe that public attention and protest saved us and that, for me personally, the best thing I could do was to not keep all my fear inside but instead to share and raise awareness of what the war on terror looks like in detail.

More information:
http://annalist.noblogs.org/category/en
http://einstellung.so36.net/en/ps/392
http://wikipedia.org/wiki/Data_retention

Bandwagons and Buzzwords

by Eric Lee
Originally published in Industrial Worker

The new technology, they said, was going to transform the Internet forever. Instead of you having to go online and "pull" web pages to your browser, it would 'push' pages to you. In fact, it was making the web browser itself obsolete. It was such an amazing thing that Rupert Murdoch's News Corporation (owner of Fox News) offered $450 million to buy the company. And companies, media outlets, even unions, were told, "you'd better get on board or you'll be left behind."

Some of you may recognize the story I am telling; it describes something called PointCast, which most of you may never have heard of. But it, and its so-called "push technology" were the next big thing a decade ago.

Most of you have never heard of it because, like so many next big things, it fell as quickly as it rose, and its massive overvaluation turned out to be a harbinger of things to come. Three years later the dotcom bubble burst and PointCast was never heard from again.

A year after PointCast peaked, another com-

Think your group needs a password policy?

1. Be Realistic: if you impose a rule that no one has time to follow, you are no better off than you were without any policies.

2. Wherever possible, let users set their own passwords. When the whole organization shares a single password, it is much more difficult to change the password.

3. Be Reasonable: be clear about why passwords matter in your organization. Is data sensitive? Is it confidential? Vulnerable to vandalism? There is a difference. If you are asking computer users to respect the confidentiality of the organization, say so. It seems less arbitrary.

4. Set an Example: never ask users to share their passwords with you. Make sure you know how to reset passwords for email, database users, etc. and let users keep their passwords private. If you are footing the bill, your ISP should have no problem resetting a user's email password if something happens and you need access to their account.

So what is the worst thing that could happen? Only you know how private your email or other files are, so there are plenty of worst things that I might not be able to list for you. On

really random passwords and don't reuse them. If you're keeping sensitive data in a web-based membership database, or if you access a shared file server remotely, you should have a truly random password. If you don't save the password, you'll find that as you type it over and over you get as used to it as any regular word. I eventually find that my random passwords are almost pronounceable.

Random password generators aren't hard to find, but here is one that I like:
`http://pctools.com/guides/password`

UChicago has a great tip sheet on passwords:
`http://safecomputing.uchicago.edu`

One good tip: use the first letter of each word in a saying or lyric that you'll remember, like "Poverty anywhere is Poverty everywhere!" becomes "PaiPe!" or "Four score and seven years ago our fathers" becomes "4sa7yaof." Be careful not to pick something that can be connected to you. For example, if you are using the first letter of the first 8 letters of the chorus of your favorite song, who knows that this is your favorite song? Have you broadcast your favorites to social networking sites?

Another good tip: when you play Scrabble (well, when I play scrabble anyhow) I can imagine all kinds of letter combinations into words. Makes it hard to play scrabble, but makes it easy to think of br2buVes as "Brought two bu Vez".

pany, an Israeli startup, called Mirabilis, had developed the next next big thing. America Online (now Time Warner) snapped up the company for a mere $407 million in 1998 and its four young owners could now retire as millionaires.

Never heard of Mirabilis? Maybe you've heard of its sole product an instant messaging client called ICQ. Or maybe not. Today ICQ is one of dozens of such products and others (such as MSN Messenger, Jabber or even Skype) seem far more popular. I wonder if anyone reading this article uses ICQ. I know that I haven't for several years.

The stories of PointCast and ICQ should be a warning to those who are willing to jump on any bandwagon and advocate the adoption of every shiny new thing on the Internet—or else face the danger of falling behind.

Here's a much more recent example: a couple of years ago, the next big thing on the Internet was the social networking site MySpace. This time, Rupert Murdoch's company did manage to purchase it for $580 million in 2005. Shortly thereafter, the site lost much of its luster as it became increasingly regarded as just another arm of Murdoch's evil empire. Today MySpace is no longer seen by anyone as being particularly "cool."

In 2005, MySpace was the next big thing. If you were serious about using the Internet, if you wanted to reach out to millions of people,

you absolutely needed to be there. But not anymore.

Now it's 2008 and there are even more bandwagons to jump on. The latest is Facebook. *(editor's note: 2009/twitter.)* Unions are being told that they need a presence on Facebook or else no one will know they exist. They need to use Facebook to mobilize thousands of people, to send a strong message to companies and governments, to grow their ranks, to make unions seem relevant to young people.

What a fantastic tool—it allows you to mobilize people online. But wait a minute—isn't this something we've been doing with websites since day one?

It is, but here's the difference. Let's say I set up a group on Facebook to tell the Burmese government to stop crushing democracy. I'll get tens of thousands of people to sign up to join my group. And I'll announce—we've got a giant Facebook group. We've got all these committed people. We're practically a mass movement.

But hang on—in what sense is a Facebook group a "group?" How does it differ from a simple online petition? The answer to the latter question is that it doesn't differ—it's just another way of doing an online petition. A worse way.

If I set up my online campaign on Facebook I can, in theory, email all members of my group. Not really, though. What I can do is to send them messages through Facebook—not to their

because my kid brother, Oliver N Hickman, was about to turn 14 and I was thinking about getting him a birthday present when I set up my first email account. For an added bonus, when I was still using that password on his 18th birthday, that was a good reminder that I should have switched passwords. Change that password every few months. At a minimum, change it once a year.

Passwords you should keep to yourself:

- your email account(s)
- the (S)FTP login for your website
- your blog login

3. Don't share private passwords. As an organization, or in collaboration with other people, you may wind up with some passwords that you can't avoid sharing between many people. Realize that these passwords are profoundly insecure and treat them as such: don't reuse your email password in a context where you'll have to share it. (S)FTP passwords and shared websites often fall into this category.

If you do share a private password, say, in an emergency, change it as soon as possible and change it in the other places where you use it.

4. There's private and then there's really private. Some things are really sensitive. If you're accountable to more than just yourself, be responsible about the passwords you choose. Use

- Newspapers and other online content
- Travel sites like Expedia, or airline sites that require you to login to search (as long as you haven't saved your credit card information!)
- Email lists, anywhere that warns you that your password will be sent to you in cleartext[1]
- Photo sharing sites (especially if you aren't using your own identity and instead using a pseudonym)

A good way to decide whether or not something is a nuisance login is this: Ask yourself, what is the very worst possible thing that could happen if someone got a hold of my password or took over my account? If your answer is "meh," it is a nuisance. If your answer is something closer to "oooh, that would not be good" you should opt for a harder password.

2. It is okay to reuse a password if you change it from time to time and only use it in secure places. For things that are private but not life or death, invent a semi-random password that you can remember. For a while I used "14ONHbro"

[1] Cleartext is text that is visible to the user. When you type in your password in a conventional password box, the text is obfuscated so that you cannot see it when you type. You see asterisks or bullets instead; that is not cleartext.

actual email addresses, but to their Facebook accounts, forcing them to login to Facebook to read my message. Even if they do this, it adds an additional couple of steps for them to follow.

If my Facebook group is over 1,000 names, I can't email them—and our experience has been that even with groups of under 1,000 names, the email doesn't always seem to work.

What you're doing by outsourcing your campaigning to Facebook is growing their company, and giving them direct access to your supporters and members. What's the alternative? Do-it-yourself online campaigns where you retain all the information on who has sent off protest messages.

At LabourStart, we have campaigned this way for years. Every time we do a campaign, we collect the emails, names and unions of participants. If they give us permission, we add them to our mailing list and they receive our weekly email newsletter. Our list has grown from 3,000 names five years ago to 51,000 names today as a result of these campaigns.

Imagine if Facebook had existed five years ago and if we had tried to campaign using it. We wouldn't have a mailing list today and we certainly wouldn't be able to send out more than 50,000 emails a week.

Facebook is a poor replacement for a real online campaigning strategy for unions. It makes us vulnerable to the whims of those who own the company. Microsoft has invested $246 mil-

lion in Facebook. It sees Facebook the same way that Murdoch saw MySpace (or PointCast) as a way to make money.

Further, unions that have tried to use Facebook have not always had such great experiences. Earlier this year, the Service Employees International Union (SEIU) tried to organize casino workers in Nova Scotia, Canada. They used Facebook and were shocked to find that their Facebook account had been closed. When they asked for an explanation they were told that they were an organization, not an individual, and weren't allowed to have an account (SEIU replied that companies were allowed to have Facebook accounts, but this had no effect).

A union in South Korea using a similar system was engaged in an organizing campaign collecting details of potential members, all of which was lost when the company shut them down.

The lesson I learn from all this is that the best tools are the ones we wield ourselves—and that the best way for unions to campaign online is not to jump on the latest bandwagon, but to spend the time, effort and money to create powerful online campaigning systems ourselves.

Pick a Good Password

by Amanda B. Hickman

In a perfect world, you would use a unique password for every password protected function that you hope to keep private. That unique password would be 14 characters long and not resemble any word in the dictionary (password is out, and so is passw0rd and pa55word). Your passwords would never be written down anywhere, ever.

Got it? Great. Now let's get real. If you are ready to be responsible about password use but can't quite get your head around the instructions above, here are some tips to make you less insecure:

1. Not every password needs to be secure: Pick one really easy password and use it only for nuisance logins, those sites where you know you won't really care if someone gets a hold of your account. Yes, someone could steal your password, but what are they going to do with it? If you're worried about protecting your privacy, use a better password, but if you aren't, use the same plain word over and over again and don't think twice about it. Good examples of nuisance logins are:

tool that isn't really useful for the need in question.

I guess my point is to be skeptical. Tools can be great, and we should use them. But we need to evaluate what tools to use, and why. We all know that the norms of the system are fucked, and that "everybody is doing it" is not an argument for anything. But it can be hard to determine what new hyped toys are worth using, and which are bogus. In some cases, it might be worth looking at offensive advertising or accepting security violations in order to reach a broader community or to simplify our organizing. But sometimes a tool only offers the downsides, with minimal advantages. We should be careful about normalizing the movement's use of the master's tools, and affirming the idea that others know what we need better than we do.

You're Evited to use the Master's Tools!

by Tufted Puffin

There are a lot of digital tools out there that offer to make our lives better in some way. What if using corporate tools could make our organizing easier? Isn't it worth using the master's tools to bring down the master?

I thought about writing a tirade on Evites, but I realized my criticism of Evites was more of a general criticism of so-called tools that we use even though they don't offer much. They may look flashy and shiny (although Evites don't even have that going for them...) and there must be some reason that so many folks use them. Thanks to technology, I can write micro-blog entries from a cell phone and share the books that I've read, websites I like, my travel plans, and every other bit of minutia about me. I've never publicized all this information before and it's not clear why it would be interesting to anybody but marketers, but maybe this is what technology is all about. Other people are doing it, so why shouldn't I?

So what about Evites? What does an Evite

offer to those invited to an event? It requires opening the Evite link to see the actual information about the event (where, when, etc.). It means anybody invited to the event can see who else is invited, if they are coming, whether they are bringing a hot date, etc. To some, this sort of voyeurism might be interesting, or even motivate them to attend an event they wouldn't have attended otherwise.

But to others, an Evite might deter event attendance. Maybe the Evite invitation has been blocked as spam, maybe going to the Evite website is a pain, or impossible if one's employer has blocked Evite. Maybe some get pissed that everybody else invited (or with the proper URL) can see that they have some tie with the organization and were invited to the event. Maybe somebody is uncomfortable attending an event if they were forwarded the Evite, and weren't themselves invited. Even if Evite does make organizing the event a teensy-bit simpler for organizers (and I'm skeptical of this), shouldn't the organizers add a bit of burden to themselves to make attendance as easy and welcoming as possible for potential attendees?

Why does Evite exist? Because some folks want to be "Your Own Personal Party Planner?" Like most so-called free web services, Evite does what it does to make money off you—they aren't doing it out of their own love of Superbowl parties or anarchist picnics. According to the annual report of IAC/InterActiveCorp, the corporation that owns Evite, in 2007 they brought in $758.5 million dollars in revenue from Evite and Citysearch. Evite presumably makes their money off ads and partnerships with people selling you shit. I don't think they currently offer paid-premium services, but maybe in the future they will. They probably aren't selling their list of email addresses to other companies, or giving them to the NSA, but maybe they'll choose to do that, too. And if the government were to subpoena them for a list of people invited to a radical event, do you think they would stand up to it? Not that the government would even need a subpoena to compile a map of social networks from Evites—it's all public information.

To further complicate matters, it's not just corporate tools that we need to be skeptical of. Many tools are developed for pure reasons, but still don't make sense for every job. I'm thinking of complicated Content Management Systems, like Drupal. Drupal is an open-source tool for building and maintaining websites. For many organizations, a Drupal site is great. But for others, it's complete overkill—it doesn't make sense to put resources into using the features Drupal provides, and instead organizations use Drupal to do what could be done just as well with a static HTML website. I see this as an example of the non-profit industrial complex, and the perceived need to professionalize organizations, but it is also an example of feeling pressure, maybe from a so-called expert, to use a