EMAIL ACTIVISM GUIDE

Movements.org

How To Recognize and Protect Yourself Against Email and Social Network Phishing

How To Use Gmail More Securely

How to Encrypt Your Email Messages with PGP

How To Send Anonymous Email Using Hushmail

How to Send and Receive Encrypted Email Messages with Thunderbird’s Enigmail

How to Send and Receive Emails Securely with Riseup

How to Successfully Harness Your E-mail List For Your Cause

PROTECT AGAINST PHISHING ATTACKS

Phishing is a way of attempting to acquire sensitive personal information such as usernames, passwords and financial information by imitating a trustworthy source in an electronic communication. It most commonly happens via email or instant messaging.

Most incidents of phishing involve using some type of technical deception (like a link) to direct a user to a site that looks and feels like the legitimate site belonging to the organization behind the email, but is actually a fraud. A lot of web browsers now have anti-phishing software built in, meaning that if you go to a site that it deems suspicious and cannot validate its security certificate, it will warn you before you can proceed to the actual site warning you that the site might be malicious. However, phishing scams have grown quite sophisticated and can be difficult to detect.

During the uprising in Tunisia, a number Facebook users inside the country discovered that their accounts were being phished by the government. According to reports, the Tunisian Internet Agency was modifying web pages by injecting them with JavaScript to steal usernames and passwords on popular sites like Google, Yahoo, and Facebook. People logging onto the sites unknowingly had their sensitive log-in information stolen. The government then quickly moved to delete Facebook accounts and groups.

With many governments stepping up their game and becoming savvier in their attempts to monitor and track dissidents online, it's important to be aware of the signs of phishing and what you can do to better protect your online accounts.

Share

Step 1.

If you receive **an email that looks suspicious**, there are a number of signs that it may be a phishing email, including:

- It usually comes from an institution or company you are likely to already be familiar with or trust, like a bank, government agency, or social networking site.

- The **greeting is usually generic** and doesn't address you personally. It may open with "Dear Customer" or "Dear [Name of company] User" rather than your first name or username.

- The email may contain **official-looking company logos and/or signatures**.

- The email **asks you to verify account information** like your username, password, or other personal information (date of birth, Social Security number, address) by sending an email or clicking on a link. It may sound something like this: *"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."*

- The email contains a link that, upon first glance, look like a valid link. However, if you hover over the link with your mouse to see the actual URL address, you can tell if it is the same link or something else. Look for any misspellings in the URL.

- You are asked to call a phone number and provide personal account information.

- There is a **sense of urgency** in the message such as: "Your account may be deleted if you do not respond in 48 hours."

Step 2.

If you believe the email you have received is a phishing attempt, there are a number of immediate steps you can take:

- Don't **reply** to the email.

- Don't download and open any **attachments**.

- Don’t click on any **links** in the email. Instead, call the company or log onto the website directly by the web address in your browser.

- **Never send sensitive personal information** like passwords, credit card information, or detailed personal information (date of birth, Social Security number, address) via email.

- **Contact the institution or company** via their support page and alert them to the potentially deceptive email. Forward the questionable email and/or take a screenshot of the page. If you forward an email, include the entire original email including the subject line and header information. Report the email to the company via their support or security contact.

Step 3.

Take the necessary steps to protect yourself against phishing in the future.

- **Use HTTPS** to access your webmail. (It’s now default on many services like Gmail).

- It’s always a good idea to **update your passwords** as well. Learn how to create strong passwords and passphrases here.

- Make sure you have **updated your browser software**. Most browsers warn you if a link you are opening could potentially be malicious because they have anti-phishing software integrated into the software. It's important to have the most up-to-date version of your browser with the latest security patches

- Make sure to **use different login names and passwords** for each of the websites you use.

- If you used Google Gmail, check out our how to guide for using the webmail service more securely.

Step 4.

As social networks have grown in popularity, the number of phishing attempts on sites like Facebook has skyrocketed. **What does Facebook phishing look like?**

- **Check the URL of the Facebook page**. Always log onto Facebook via a legitimate domain https://www.facebook.com. Don’t log into Facebook if it is a similar but different domain. A fraudulent website may include the term Facebook before the domain (.com). This is called a subdomain. For instance, the address facebook.com.profile.a340ah3.com looks legitimate, but if you look more closely, the domain is actually a340ah3.com not facebook.com

- Be suspicious of any link, message, wall posting, or pop-up window that requires an additional login or asks you for your personal account information. Remember, **a phishing attempt could come from one of your Facebook friends** whose account has been compromised.

Step 5.

If you believe your account is being phished or you receive a suspicious link, message, post, or pop-up window that you believe is phishing:

- **Report** it to Facebook by sending an email to privacy@facebook.com. Visit the Facebook Help Center to get more specific help regarding your account.

- **Don't click on any links** in the post or message.

- **Never send sensitive personal information** like passwords, credit card information, or detailed personal information via a Facebook message.

- **Change your password** immediately. Learn how to create strong passwords and passphrases here.

- If the message or post comes from a Facebook friend, immediately **contact that person** to let them know that their account has been compromised. The same goes for a message or post coming from a company or oraganization you follow on Facebook.

- Share this knowledge with your friends!

Step 6.

Take the necessary steps to protect yourself against Facebook phishing in the future:

- **Enable HTTPS for Facebook.** In the case of Tunisia, experts found that the embedded JavaScript only appears when Facebook was accessed with HTTP instead of HTTPS, underscoring the importance of using HTTPS whenever you log into social networking sites.

- Always make sure you are logging onto Facebook via a legitimate domain.

Step 7.

- If you have given out your personal information and believe you've been the victim of phishing, check out the Anti-Phishing Working Group's advice on what to do.

USING GMAIL SECURELY

Gmail, Google's free webmail service, is wildly popular. As of November 2010, it had 193.3 million monthly users worldwide. It's easy to use, has a convenient chat feature, and is linked to Google's other products. In a smart move last year, the company made Gmail more secure by allowing for HTTPS access by default. If you use Gmail for day-to-day personal or professional correspondence, there are a number of steps you can take to use the service more securely. Have your own tips? Share them below!

Remember, though, if you are looking for the safest way to send encrypted email, PGP is definitely your best bet. Hushmail is another tool available to send anonymous email.

Share

Step 1.

Always access Gmail directly by going to https://mail.google.com. If you are on your mobile device, go to https://m.gmail.com.

Gmail now uses a secure HTTPS connection by default. This means that email is encrypted as it travels between a user's browser and Google's servers.

Step 2.

Read up about Gmail's privacy and security. Familiarize yourself with Google's policies and the protections they offer. Visit Gmail's Security Center and **complete the Gmail security checklist to make sure your account is secure**.

Step 3.

Never give out your password to anyone. Remember that Gmail will never ask for your username or password, so if you get such a request, it's bogus.

Step 4.

Do you use any Gmail-related plugins or extensions? **Google can't guarantee the security of these third party services**, so be careful when using them or avoid downloading extensions all together.

Step 5.

That said, there is **an extension available for signing and encrypting Gmail messages**. The Gmail S/MIME extension for the Firefox browser allows you to send and receive signed and encrypted messages in Gmail. S/MIME stands for Secure/Multipurpose Internet Mail Extensions.

Gmail S/MIME adds a lock icon to the Gmail compose and reply screens. Initially this lock will be shown unlocked. After you enter the recipient's email address, the lock will change to the locked state if there is an entry for that user in the Firefox certificate database. Learn more here.

Step 6.

Make sure to **regularly update both your operating system and your browser(s)** to fix bugs and add security updates.

Step 7.

Use a strong passphrase and change it frequently. Unlike a password, a passphrase is usually longer (at least 20 characters) and much harder to break. Make sure this passphrase is unique to Gmail; don't use the same passphrase on different sites. See our how to guide to learn more about creating strong passwords and passphrases.

Step 8.

Update your account recovery options. In the event that you forget your password, you can set up options to recover it.

Log into your account at https://www.google.com/accounts and click Recovering your password under Personal Settings. You can add a recovery email address--another email account you use that Google can send alerts to if you lose access to your account--and your mobile number so an SMS with a recovery code can be sent to you.

Step 9.

Check what third-party websites are authorized to access your Google account data.

Log into your account at https://www.google.com/accounts and click the My Account link at the top right of the page. Click **Authorizing applications & sites** to see a list of all third-party sites you've granted access to. Click the **Revoke Access** link to disable access for a particular site.

Step 10.

For email attachments, select "View as HTML" rather than "Download." The contents of the attachment will then appear in a new browser window rather than being downloaded to your computer. Excel file attachments can also be opened in Google Spreadsheets and Word, PowerPoint, and Adobe PDF files can be viewed in Google Docs Viewer.

Step 11.

If you do need to download an email attachment, **make sure you have an anti-virus software installed and updated**. Run the software against any email attachment that you want to download.

Step 12.

Each time you log into Gmail, **check the details about the last time your account was accessed**. Scroll to the bottom of your Gmail page and you'll see: "Last account activity: X hours ago on this computer. Details." Click on the "Details" link.

You will then see the IP addresses of the computers that have recently accessed your accounts. Anything look fishy? Do you see any unusual IPs that are not yours? Does it appear that someone else may have accessed your Gmail account?

Step 13.

Clear your cache and cookies regularly, especially if you are using a public computer.

Each time you access a file through your web browser, the browser caches or stores it. This makes it easier for the browser to retrieve data while you are surfing the web. A cookie is a file created by a web browser that is stored on a computer and is used for a number of reasons from authentication to shopping cart contents.

How you clear your cache and cookies depends on the type of browser you use. Learn how here.

Step 14.

Finally, **always always always sign out after you've finished your session**, especially if you are using a public computer.

Share

USING PGP TO ENCRYPT EMAILS

PGP, which stands for Pretty Good Privacy, is a software that can be used to encrypt data on your computer. It provides both **cryptographic privacy** and **authentication** to secure your data. Cryptographic privacy is the art of protecting information by transforming it (encrypting it) into an unreadable format. Only those with the correct key can decipher/decrypt it into plain text, a readable format. Authentication is used to establish and confirm identification and association.

The **freeware version** of PGP allows you to encrypt and sign email messages and individual files that you exchange with others. **It only includes PGPmail.** To use other components of PGP, like email plug-ins for email clients like Outlook or whole disk encryption (PGP Whole Disk), you will need to upgrade/buy PGP license and software.

PGPMail allows you to encrypt and sign email messages and individual files that you exchange with others. If you are sending or receiving emails with sensitive information, you may want to better secure the messages by encrypting them.

Share

Step 1.

You can purchase PGP onilne for $149 USD. A **freeware** (also known as shareware) version of the software is also available for non-commercial use. It is called trialware on the PGP site, but it's still freeware. According to creator Philip Zimmerman, PGP will revert from full-featured trialware to freeware after 30 days.

Point your browser to http://www.pgp.com/downloads/desktoptrial/desktoptrial2.html.

Step 2.

Read and accept the PGP Software License Agreement. You will then be re-directed to the download page.

Download the software for your particular operating system.

Step 3.

Double click on the file and you will be guided through the steps to install PGP on your computer.

During the installation process, a dialog box will appear asking ou to select which PGP components to install. **Uncheck all of these boxes if you want to only use PGP as freeware.** You won't be able to actually use any of the components listed in the dialog box unless you buy the software and obtain a license.

To finish installation, you will need to reboot your computer.

Step 4.

After the installation of PGP Desktop completes and your computer reboots, you will be prompted to enable PGP for the account. A PGP License Authorization box will appear.

If you want to **authorize this trial**, enter the following information.

Enter **Trial User** as the user name and **30 Day Product Trial** as the Organization.
Do not enter an email address.
Enter this license number: **DKCE2-C6RQL-VLCBG-AC494-NBFG0-E6A**.
Follow the remaining instructions onscreen to complete installation.

If you only want to use PGP as freeware (recommended), don't enter anything into the field boxes, and just click "Later."

Now you are running PGP freeware!

Step 5.

PGP is accessible through the **PGPtray icon** in the system tray area.

The PGPtray contains the tools you need to operate PGP on your system. Click on the tray icon and you should see a menu with following options: Hide, About PGP, License, Help, Options, PGPkeys, PGPmail, Current Window, and Clipboard.

Step 6.

First, you will need to **create a public key**. Select PGPkeys from the menu. Generate a key by choosing "Keys-New Key" from the PGPkeys menu, or by clicking on the Key icon. The key generation wizard will launch. Click "Next."

The text that you enter into the "Full Name" and "Email address" fields will be associated with your key and distinguish it as belonging to you. You do not actually need to use your own name there, but you do need to use a valid email address. Click "Next."

Now you will choose your passphrase. **Choose a very strong passphrase that includes upper and lower case letters, numbers and characters.** Don't forget this passphrase!! If you forget it, you will not be able to use the key to decrypt anything!

Retype the passphrase for confirmation, then click "Next." The key will be generated, then click "Finish." The PGPKeys window will appear. You should see your public key in the window. **Write it down!**

Step 7.

After you have created your public key, enter the PGP option inside the control panel, type your PGP key into the box, and click "Add."

Step 8.

Distribute your public key to people! Email it to them, call them and give it them, etc.

Step 9.

Get other people's public keys. Ask people you are corresponding with for their public keys.

Step 10.

To sign and/or encrypt an outgoing email message: Compose your email message as usual. Then click on the PGPtray icon. Select "Current Window-Encrypt," "Current Window-Sign," or "Current Window-Encrypt and Sign" depending on what you want to do. PGP will process the message replace your message in the composition window with the encrypted message. You can then send the processed message in the usual way.

Step 11.

To decrypt a received message: Open the message, then click on the PGPtray icon. Select “Current Window-Decrypt and Verify.” If the mailer does not support window operations, then PGP can still be used by manually moving data to and from the clipboard. After composing the message, select the entire message and copy the text to the clipboard.

ANONYMOUS EMAIL WITH HUSHMAIL

Worried about sending an email from your personal account and wish you could send one anonymously? Look no further than Hushmail, a **free and open source anonymous web-based email service**. You **don’t need to install anything** to use Hushmail. Just sign up for a free account and you are ready to go.

Hushmail’s free email account provides 2MB of storage and an ability to send PGP encrypted email to anyone. PGP stands for Pretty Good Privacy and provides both **cryptographic privacy** and **authentication** to secure your data. Cryptographic privacy is the art of protecting information by transforming it (encrypting it) into an unreadable format. Only those with the correct key can decipher/decrypt it into plain text, a readable format. Authentication is used to establish and confirm identification and association. All mail traffic is protected with HTTPS as well.

Share

Step 1.

Point your browser to http://www.hushmail.com/

Step 2.

Click on “Sign up for free email.”

Step 3.

Choose your new email address or let Hushmail automatically generate one for you. **Remember, don’t include any personal information in your email address.**

Step 4.

Choose your passphrase (password) for your email account. Create a **strong password** using a combination of upper and lower case letters and numbers. Re-type the passphrase. Learn more about creating strong passwords by checking out our how-to guide.

Step 5.

Type in the numbers in the box for verification purposes.

Step 6.

Check the boxes that you have read Hushmail's terms of service and are not using Hushmail for illegal services.

Step 7.

Click "Create account now." You will then be directed to a confirmation page that your email account has been created.

Step 8.

Write down your hushmail email address and passphrase and store them somewhere safe.

Step 9.

Click on the button "To sign in now, click here." You will be re-directed to the Hushmail homepage. In the upper left corner, you will see "Sign in to webmail." Enter your full hushmail email address and click "Sign In."

Step 10.

You will be asked if you want to upgrade to a premium Hushmail account. You can either go to your free account or pay for a premium account.

Step 11.

You will then be asked to provide the passphrase you created. Enter it into the box, then click "Authenticate."

Step 12.

You will now be directed to your Hushmail email account. On the top of the page, you will see menu items:

Check Mail: Refreshes your account and checks for new mail.

Compose: Create a new email message.

Contacts: Manage contacts.

Spam Control: Manage spam.

Preferences: Set preferences. Note: This is where you can enter a name you want associated with outgoing email, add access instructions for external email accounts, change your passphrase, and export encryption keys.

Hushtools: Use Hushtools to encrypt and/or decrypt email messages, and create digital signatures.

Help: Find help for problems you are having with Hushmail.

Quit: Sign out of Hushmail.

Step 13.

Compose an email by clicking "Compose" at the top of your screen. A pop up window will appear where you can add the recipient(s)'s email address and compose your email.

Click "Send" when you are done.

Tip!

After composing your email, click "Message Options." **Make sure the box is checked next to "Encrypt Message" and "Sign Message."** If your message cannot be encrypted forthe recipients of your email, you can type a question and answer for your recipient. Your recipient will need to know the answer to your question to be able to read the email.

Tip!

You can access your Hushmail account on your mobile phone. Point your mobile browser to m.hush.com.

ENCRYPTED EMAIL WITH THUNDERBIRD ENIGMAIL

Worried that the email you are sending and receiving is not safe? Enigmail is a security extension to Mozilla Thunderbird and Seamonkey that enables you to **write and receive email messages signed and/or encrypted with the OpenPGP standard**.

Enigmail uses public key encryption to make your email communication more **secure**. You can send confidential emails to anyone who has sent you their public key. The owner, who has a private key that works with the public key, will be able to access and read the emails sent.

What do you need to use Enigmail?

Enigmail is an **plugin** or add-on for Firefox. It cannot be run by itself. To use Enigmail, you will need to install the GNU Privacy Guard (GnuPG). You may also need to install the proper

Enigmail language pack. You will also need to download Mozilla's free and open source email client, Thunderbird. http://www.mozillamessaging.com/en-US/thunderbird/

Share

Step 1.

Before you can use Enigmail, You need to install the GNU Privacy Guard (GnuPG). Point your browser to http://www.gnupg.org/. As you run the installation, you will see the Choose Components screen. Leave all of the boxes CHECKED. Click "Next." Continue through the installation process.

Tip!

Visit Enigmail's Quick Start Guide for help installing GnuPG on your computer.

Step 2.

Download Thunderbird. Check out Tactical Technology's helpful guide for learning how to register your email account (such as Gmail or Riseup) with Thunderbird.

Step 3.

To get the Enigmail add-on, point your browser to http://enigmail.mozdev.org/home/index.php. Click on the link to download the file and save it to your desktop.

TIP!

Make sure you have already downloaded the Firefox web browser!

Step 4.

Open the Thunderbird file you have download to your desktop. In the main window, you will see "Tools." Click on this, and then select Add-ons.

An add-ons screen will appear showing all of your Thunderbird plug-ins. Click the "Install" button on the bottom left of this screen. Select the Enigmail file you saved to your desktop, then click "OK."

An installation screen will pop up. Select "Install Now."

The add on will be installed, and you will be asked to restart Thunderbird. Click "Restart Thunderbird." After Thunderbird restarts, you should see "OpenPGP" on the main menu bar.

Step 5.

To make sure all the components are working, Select “OpenPGP” from the Thunderbird menu bar and select “Preferences.” Under “Files and Directions” you should see *GnuPG was found in...*

If Enigmail was not installed properly, you will receive an error message.

Step 6.

Now **configure your email account**(s) to use Enigmail.

Select Tools, then Account Settings.

On the left sidebar, under Work Account, select OpenPGP Security. Check the box next to “Enable OpenPGP support.”

Select the radio button next to *Use email address of this identity to identify OpenPGP key.*

Click OK.

Step 7.

Now it is time to **create your first key pair**.

As they note on their website:

“Enigmail uses public key cryptography to ensure privacy between you and your correspondents. In public key cryptography we use two different kinds of keys to give us confidentiality and assurance. By 'confidentiality' we mean that only the people you want to read a message will be able to read a message. By 'assurance' we mean that people who read messages from you can be sure that it really came from you....All you need to understand is that you will be creating a *public key* and a *private key*. The public key can be shared with the whole world--friends, neighbors, relatives, enemies, even intelligence agencies. But you need to guard the private key very, very carefully.

Start Thunderbird.

Start the Enigmail Key Manager by clicking "OpenPGP" in the menu bar of the Thunderbird main window. Select "Key Management".

When the Enigmail Key Manager opens, click on "Generate" in the menu bar and select "New key pair". A new window will pop up.

At the top of the window, tell Enigmail which email address to associate the key pair with b selecting whichever account will be receiving encrypted mail.

Choose your **passphrase** and enter it into the box next to Passphrase. You will need to add it a second time to make sure it is correct.

Click “Generate Key.” Voila! You now have a key pair!

Step 8.

You will now need to locate your Key ID. This is a sequence of eight letters and numbers used to identify your key.

Start the Enigmail Key Manager by clicking "OpenPGP" in the menu bar of the Thunderbird main window. Select "Key Management". Enter your email address in the search box. The key you just created should appear, and over at the right you'll see your key ID. Write this down; you'll need it.

Step 9.

Share your key! The easiest way to share your public key is to publish it on the *public keyserver network*, a global database of keys.

Click on your key in the Key Manager.

Then click “Keyserver.” Select “Upload public keys.” Enigmail will ask where it should send your key. Use Enigmail’s default, pool.sks-keyservers.net, and click “OK.”

Step 10.

Test out Enigmail by writing your first signed piece of email.

Since not many people use Enigmail, Mozilla recommends sending a signed or encrypted email to Adele [adele-en@gnupp.de], the "Friendly OpenPGP Email Robot". Adele accepts OpenPGP messages and replies in an explanatory way to any kind of OpenPGP messages. Don't forget to attach your own public key if you send your first email to Adele. You can use the menu *OpenPGP -> Attach My Public Key* for this.

Write an email in plain text.

Tell Enigmail to sign it by clicking on the “OpenPGP” button. Make sure the “Sign” option (and ONLY this option) is checked.

Hit Send. You will be prompted to enter your passphrase. Enter it. Now your email will be sent!

Step 11.

To send an encrypted email to someone, **first you will need to ask him or her for their key ID**. Write it down.

Now, open the Enigmail Key Manager, and then click on "Keyserver --> Search for keys".

Enter the person's key ID in the search box, prefixing it with "0x", if necessary. For instance, if someone were to tell you their key ID was "AYM007, you'd enter it as "0xAYM007".

Click OK. Enigmail will search through the keyserver and look for the key you want. If Enigmail finds it there, it will be added to your own local copy of keys.

Now, you are ready to write an email. Compose an ordinary email. Before you send it, click on the OpenPGP button. Select “Encrypt.” Then hit Send.

If the email address of your message matches an address on your keyring, there's nothing more to do; **your message will be encrypted and sent on to your correspondent.** If there's a problem with the matching, you will be asked to manually select a key from your keyring. If you see this menu, then simply select the proper keys and you're done.

Step 12.

Enigmail will automatically try to decrypt any encrypted email you receive by asking you to enter your passphrase.

SECURE EMAIL WITH RISEUP

Riseup is a **private and secure e-mail service** that allows you to send and receive e-mail over the Secure Sockets Layer (SSL) encrypted connection. You can access your e-mail account via the internet or through an e-mail client program. Riseup recommends using Thunderbird. Learn how to download and set up Thunderbird here.

Share

Step 1.

If you know two people that already have Riseup accounts, **ask them to give you an invite code**. You will need two total invite codes. You must get the invite codes before you begin filling out the request form. You cannot go back and add them in later.

Don’t know anyone using Riseup? **Don’t worry—you can still request an account.**

Step 2.

Point your browser to https://mail.riseup.net/ and click on “Request Account” under the main logo.

Make sure your connection is secure; your web address should read “https://” (the s indicates SSL) and you should see a green text message stating “Your connection is encrypted” on the left above the login field.

You will walk through the steps of requesting an account. Have your invite codes ready. If you don’t have invite codes, go through the request process, and wait for Riseup to approve your request, which may take a few weeks.

You will need to accept Riseup’s social contract, privacy policy, and terms of service. Then you will be asked to provide a username, which will become your e-mail address. For example, if the username is “movements” then the e-mail address will be movements@riseup.net

Fill out an alternative e-mail, display name, language, country, and time zone. Click "Next."

Then you will be asked to write a security question and answer, as well as a password for your account. Click "Next."

You now have the option of offering a monetary contribution to Riseup. Your decision to contribute or not contribute does not affect your account registration process. Click "Next."

Enter the invite codes you received from two Riseup account users.

Click "Finish." You will see a notification that your registration process was successful. Click “Return Home” to go back to the homepage.

Tip!

Riseup works best with the Firefox browser.

Step 3.

If you have successfully created an account and been approved, you can log in on the main page.

You have two different login options, and there is no major difference between the two. Squirrel Webmail is best for English interfaces, while IMP Webmail is best for non-English interfaces.

Type in your username and password. With the IMP Webmail, you have the option of selecting your language. Click “Log in.” You will then be directed to your account.

Tip!

If you are accessing your account from a public setting and do not want to type in your password, under the Squirrel Webmail login, type in your username, then click the link for “virtual keyboard” before entering your password. A virtual keyboard will be activated that you can use to enter your password.

Step 4.

Want to **change your account setting**s? Point your browser to https://user.riseup.net/ and login to your account. You will be directed to your control panel.

Click “My Settings” on the left panel. Change any account details you want, then click “Save changes.” Remember, if you change your username, this will change your e-mail address!

Click “E-mail” on the left panel to access your e-mail control panel. On this page, you can manage the maximum size of e-mails (quota) for your mailbox. A quota is the amount of disk storage you are allowed on the mail server.

You can also add aliases for your e-mail account. Aliases are additional e-mail addresses that your account can use to receive mail. You can share an e-mail address to forward your riseup.net e-mail to as well. Click “Save Changes.”

Tip!

Change your password every few months! All you have to do is type in a new password and then click “Save Changes.”

Step 5.

Want to share an invite code with someone? Click “Invites” on the left panel. On the Invites screen, click “Create a new invite code” to generate an invite code. You can then print the code or write it down to give to someone else.

To exit the control panel, click “Logout” on the bottom left.

How to Successfully Harness Your E-mail List For Your Cause

Posted *by*Susannah Vila in Build Awareness , Email Advocacy, Keep Supporters Engaged

Collecting email addresses and using them to **mobilize** your supporters is one of the simplest but most important tactics for online organizing.

As Ricken Patel, founder of Avaaz, told us, “**Someone operating out of their bedroom can do this better than a multimillion-dollar organization with a huge staff**.”

Before you get started, though, look over these tips for how best to turn a list of e-mails into a powerful tool for activism.

Share

Step 1.

You are communicating with people online in order **to serve them, not you and your organization, so begin by asking your membership what they care about most.** Why do they support your cause? What are their goals and ideas of success regarding the cause?

Don’t send out **any** e-mails before you understand what your members care about.

Tip!

Ask people on social networks, use free survey services like Survey Monkey, or use mobile phones.

Step 2.

Write your first e-mail. If you’re lucky, people will read the subject line and the first sentence, so put as many important words in this space as you can—**lead with a fact or recent news story that will provoke emotion**—and make sure that a link is immediately visible.

Tip!

The names attached to your e-mails should be authentic and trusted by your membership. **Consider having the e-mails come from your director rather than the name of your organization**.

Step 3.

What's the action you want to get out of the e-mail? Each e-mail sent out should have one clear action associated with it.

Do you want the receiver to click on a link? Then include it two or three times within the e-mail, and make sure each link takes the reader to the same page.

Are you publicizing an event? Remember to include all pertinent information including time, location, and directions.

Step 4.

Keep your e-mails **short and to the point**. Just as you must grab people's attention with the e-mail subject line, you must be able to clearly share your message in the short amount of time that they have to read your e-mail.

Tip!

Switch it up; don’t always ask people for the same thing.

Step 7.

Decide when, and how frequently, you will be sending e-mails. Try setting up an e-mail calendar with, for example, one message per week, and stick to it. The only exception is if your cause ends up in the news or if a time-sensitive action arises. In this case, you should break your schedule and send e-mails with more frequency. **People will be more receptive to your e-mails if the issue you are addressing is in the news.**

Send e-mails in the morning when people are more likely to be checking their inboxes. Avoid Fridays!

Tip!

It seems obvious, but it should be emphasized: Don’t send too many e-mails!

Tip!

Everyone wants to make a difference. Your job is give them the right story, one that is true and credible, to convince them that the world can change and that they can change it. Don’t spend too long talking about a problem without offering a solution.

Step 8.

Poll again (and again, and again) and check analytics. Always check back in with your supporters.

Step 9.

Set goals for your e-mail campaigns, and use analytics to gauge your success with regard to those goals. How many people clicked on the link you put in the e-mail? If you sent one e-mail at 10 a.m. and one at 4 p.m., which one was opened and clicked on with greater frequency?

Step 10.

Develop relationships between the sender and the receivers. A real live person with a name rather than an organization often does a better job of grabbing people’s attention.

If there are at least a few of you and you have different roles within your group or organization, consider creating “e-mail relationships” with your membership base so that e-mails on a certain topic always come from Joe B. while e-mails on another topic come from Suzy S.

Tip!

Make sure that your e-mail **reads like a conversation**. The e-mail comes from a real person, so make it sound like a real conversation! Don't be afraid to use a specific voice or personality.

Step 11.

Follow through. If someone signs up for your e-mail list, it means they are at least somewhat interested in your work. If someone takes the action asked of them in the e-mail, it means they are more interested—don’t waste that opportunity. Ask them immediately to help with something else. For example, ask your supporter to tell a friend about your cause, to follow you on Twitter, or to attend an event.

Write out a list of actions that you will ask of your e-mail list. You should identify an action for the first time signups, and action for those who received their first e-mail and took the action asked of them, and so on...

Step 12.

Is there an e-mail address users can reply to when receiving an e-mail blast from your organization? Make sure that they can click "reply" and reach a real person at a functioning e-mail address.

Step 13.

Do you publish a weekly news roundup or a monthly newsletter? Send this information to your e-mail list!

Step 14.

When you receive new e-mail signups, don't just dump them into the regular list. Send them a welcome e-mail describing the campaign/organization and what to expect. Without this context, the regular e-mails that you send them will not be as powerful or compelling.

Movements.org