Email Security

Protect your email data and accounts

zimbra®

A SYNACOR PRODUCT

Email Security

Protect you email account and data

Identity theft, fraudulent use of your credit card, ransomware… Cybercrime is always evolving.

There are some simple things you can do to protect your email data and accounts. How can you protect yourself from the most common and real threats like:

- Identity and credit card information theft
- Theft of proprietary data
- Precise phishing attacks
- Ransomware
- Malicious attachments
- Being hacked

Secure your account

Compromised accounts are still one of the biggest security problems. In the past, criminals mainly used hacked accounts to send spam. Now these accounts are being used for spear phishing attacks.

Criminals monitor an account to gather information and get access to the account calendar, contacts and historic email. Criminals wait for the right time, then craft an email with seemingly legitimate information asking your co-workers or family members to send confidential information or make a money transfer. Do not underestimate these criminals. Their phishing emails can fool anyone.

Secure your account using:

- 2-factor authentication (2FA)
- A passphrase rather than a password
- Caution

I-likeCoffee@4AMinthemorning
Easy to remember, hard to crack!

2FA is an extra layer of account safety, much like having two locks on your front door. 2FA is available for all editions of Zimbra. With 2FA, you provide your user name, password and a one-time access code (generated by an app on your phone) to log into your account.

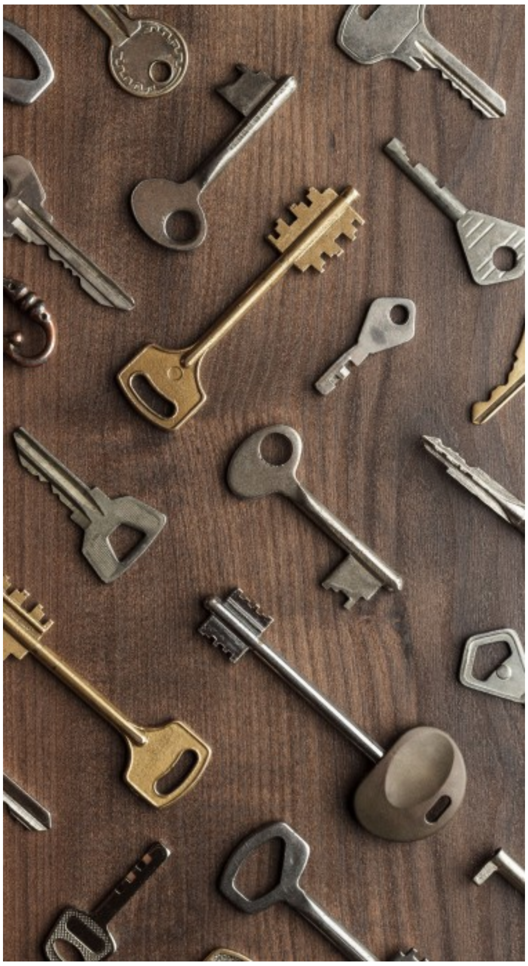
Passphrases are easier to remember than complex passwords. A passphrase is also hard to crack. You can use a passphrase instead of a password the next time you need to set-up a new password. An example of a passphrase: I-likeCoffee@4AMinthemorning.

Be cautious! If you receive an email with an invoice or a link to make a payment, contact the sender via phone to validate the legitimacy of the request.

Email Security

Protect you email account and data

Secure your communication



Email messages and attachments can be intercepted as they are sent over the Internet. Many email providers support secure connections for incoming and outgoing email. However, the email protocol has a flaw: it falls-back to unsecure connections if an error happens. Hackers use this flaw to read or alter email messages without you knowing. Hackers can also get access to recipients' accounts and read email there.

Secure your communications using:

- S/MIME
- PGP
- Links to share attachments
- Email via a secure-email service

S/MIME and PGP provide encryption and digital signatures for your email. If you use encryption, only the intended recipient can read the email. Digital signatures ensure no-one has tampered with or read your email.

S/MIME: The user needs to buy a TLS Certificate from a Certifacte Authority (company).

PGP: The user needs to generate a keypair. A keypair has a private key, which should be stored in a secure place, and a public key. The private key is used to decrypt messages. The public key is what your contacts use so they can encrypt email to you.

Both methods are slightly complex to understand for most users, so do not be discouraged if you have trouble implementing these features and ask your support team if you run into problems.

Instead of sending attachments, share documents via a link in Zimbra. This allows you to set an expiration date and/or set a password on the link for some control over the document after the email is sent.

There are also online email security services to add encryption, perform additional virus and malware scanning and add two-factor authentication.

Email Security

Protect you email account and data

Back it up!

Take a moment and analyze what email, documents and other digital data are most important to you. Make backups of this data yourself. Your (cloud) provider may not have backups or may be unable to restore them quickly. Zimbra has many backup features that administrators can use to secure your data, but consider doing so yourself as well. Zimbra has an export feature that creates a zip file of all your account content. Store this data offline in a safe place. Secure your data!

Email and Internet safety checklist

Here are some more things you can do to protect your data:

- Consider your email and IM contents before clicking Send. Should the content be shared outside of your organization? When in doubt, ask before sending!
- Avoid the use of public Wi-Fi. Only use Wi-Fi at work and in your own home.
- Disable Bluetooth on your devices when not in use.
- Keep your phone, computer, routers and all other Internet connected devices up-to-date and change the default passwords.
- Be careful and selective about what you download to your computer from the Internet.
- Reset your Internet browser to factory settings periodically to remove any accidentally installed plug-ins or extensions and clean up tracking cookies and other processes that may run in the background.
- Avoid the use of browser extensions if you can.
- Use passphrases and passwords that are unique and do not re-use them for other accounts.
- Consider using email encryption.
- Always lock your screen if you walk away from your device.
- Do not leave your device unattended.

Do not ever:

- Open an email from an unknown address.
- Click a link in an email unless you expected someone to send it.
- Open an attachment unless you were expecting it or it was from an unquestionably trusted source. Scan any attachment before you open it!

zimbra®
A SYNACOR PRODUCT

SYNACOR