Securing your Email

Technology with Integrity

By Tim Torian, Torian Group, Inc.

Summary:
Attacks on your email account are a growing problem. Protect your Email account from hackers by using 2 factor authentication. Use a secure and reliable Email provider. Make sure your email is backed up.

Email allows people to do business with you - it contains critical business information. You probably rely on your calendar and contacts to stay organized. Your email address is linked to other services and website logins which are often critical to you.

Picking the right email provider is the first step in securing your email. For most businesses we recommend Outlook with Exchange Online (Office 365). We have a separate article on selecting an email provider – ask if you are still considering options.

Exchange Online is a mail service provider – they store your email, and handle sending and receiving email. It is part of the "Office 365" suite of online services. The Email client is what you use to interact with the email provider. For most businesses this is Outlook.

Exchange (Office 365) email is hosted on Microsoft servers, and is backed up by them. They have a lot of protection in place, including redundant servers in multiple geographic locations. They are unlikely to lose the entire mail store due to a failure- It's not impossible, but very unlikely. They have a dedicated staff working on security and safety. Their servers are unlikely to get infected or encrypted. Unless the entire Microsoft email server system is compromised, your email store is fairly safe. However - Microsoft DOES NOT BACK UP YOUR EMAIL. You can't ask them to restore the contact or message you accidentally deleted last month.

A more significant risk is that someone will get in to your email by getting your password. This can happen with a brute force attack - simply trying to log in to the account with a dictionary of passwords, until one works. It can also happen if you use the same password as your email on other websites – the site gets hacked, and the hacker tries the password on your email account. (you can check your email at www.HaveIBeenPwned.com to see if it was in a known data breach.)

If a malware program or hacker can manipulate Outlook or your webmail, you have a problem. They can start recovering passwords to your bank and credit card accounts, send out malware to your contacts, and do anything you could with your email. Worse yet, you may lose access to your account when they change your email password.

You need to protect your login and have a backup of your mail data.

Protecting your email login

You can protect your login by setting up additional login security on the account, called "2 factor authentication". It is simple to set up, and we strongly recommend it.

Each PC or phone/tablet gets a unique "token" which gets installed in Outlook and replaces the password. It only works on that device, so can't be used to log in to the account from elsewhere. You open Outlook normally once it is set up – no extra work is needed to log in. This must be set up locally on each device, so requires an onsite visit.

In addition, a second device - usually a smart phone or tablet - gets set up as the "Second factor" for logging in to the account from the internet (Outlook Web access, or Office 365 online). When you log in via a browser, your phone or tablet pops up a message asking you to confirm that it's you. This prevents anyone from attacking or using your password over the internet. Each User account requires a second device, which can be either their smart phone, or you can set up on a company tablet used for that purpose. One device can be used for multiple accounts if desired.

Protecting your email content

Email that you delete goes to deleted items. Emptying the deleted deletes message permanently. There is a window for recovery of 14 days (default "deleted items retention time"- configured on the server) which allows an administrator to recover email for a limited time. There is a risk is that you will accidentally delete contacts or calendar entries – these will immediately get deleted. We have had this happen. If permanently deleted (cleared from deleted items) - it's gone.

Once email is received, it doesn't get changed – it can be forwarded, deleted, etc. but not modified. Unless it arrives infected, an individual message is not likely to be infected or encrypted by malware. However, your PC or device can be infected, and the entire local mail data file can be deleted, infected or encrypted. This is unlikely to result in loss, because your email client (Outlook) won't be able to read the file, and therefore won't update the server – the server's copy will remain good. Once the PC is fixed, you can reconnect to the server and to your email.

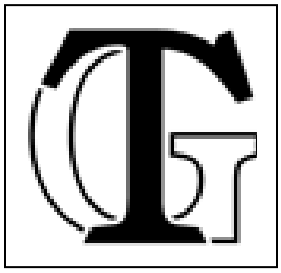
Recent versions of Outlook allow you to choose how much of your email gets "cached". This local store is a copy of your email, and we recommend you turn it on and set it to download all your email (in the email account settings).
If there is a device with a local copy of Outlook which was turned off, you can sometimes recover the missing content by deliberately disconnecting the device from the internet before opening Outlook. It will still have the local copy.

To avoid losing your email, back it up. Backup solutions fall into 2 categories: backup the email content on server, and/or back up the email copy on the PC.

We have used Skykick backup to back up the server data every few hours. It is set up on the Exchange Server, and just works. Cost is about $5/Month per email account.

Workstation backups will get a copy of the local Outlook email data file if Outlook is closed when the backup runs. The cost for a managed full PC backup (local and offsite) is $10/Month. We monitor it along with the managed services to be sure backups are working. It's sometimes challenging to get staff to remember to close everything nightly and leave the computer running to assure a good backup. Logoff can be forced at a certain time nightly if you are on a domain. To get the local backup, a second "backup" hard drive can be added to the PC.
The PC backup is a better option, as it protects all your local files in addition to email.

Give us a call to assure your email is protected properly.



Tim Torian has his degree in Computer Science, and has been consulting on technology for business for the past 30+ Years. He has multiple industry certifications including Microsoft and Cisco. He has taught computer networking at the College of Sequoias and Cal Poly Extension. He was awarded "Entrepreneur of the year" by the Tulare County EDC in 2008. Torian Group was awarded "Technology Business of the Year" by the SBDC in 2011. He is president of Torian Group, Inc. which provides a full range of Technology Consulting services to local business, including computer services, networking, and network design. www.toriangroup.com