EMAIL SECURITY CHECKLIST FOR RIAS

Email is one of the biggest threats to your RIA. It's the most common way hackers access your network and its a big potential source of data loss and employee error.

8 Email Security Protections Your RIA Should Have in Place Now

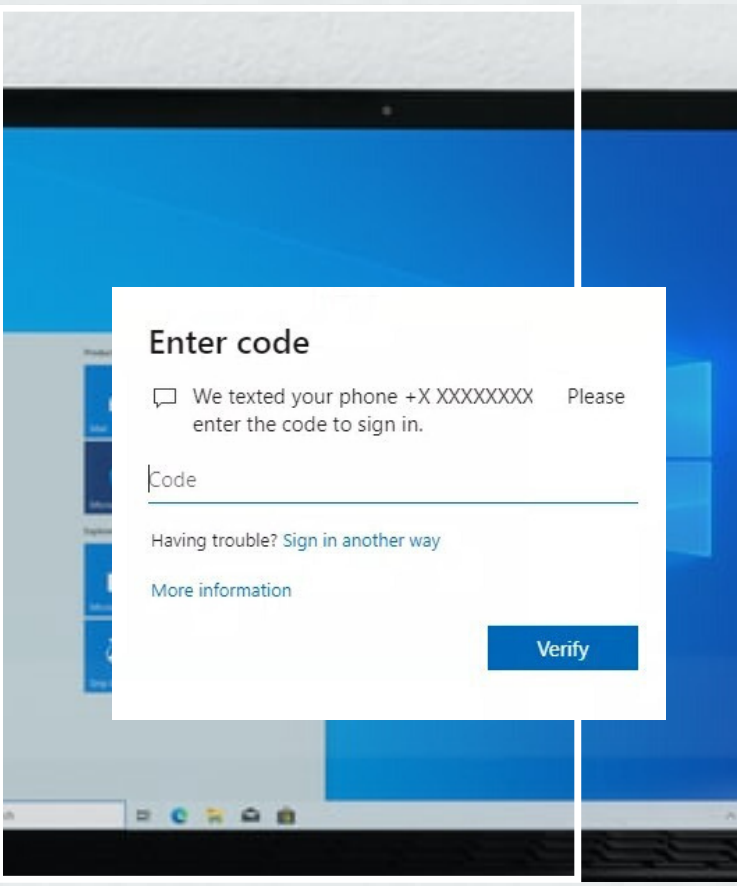
(Especially if you're using Microsoft email)

If you're like many other RIAs, chances are you can't give a confident "Yes" to these questions. You might be missing a few critical pieces without realizing it.

The following email protections are available with your Microsoft 365 license but need to be configured properly. If you don't know the answers to these questions, you might be taking a big gamble with your email.

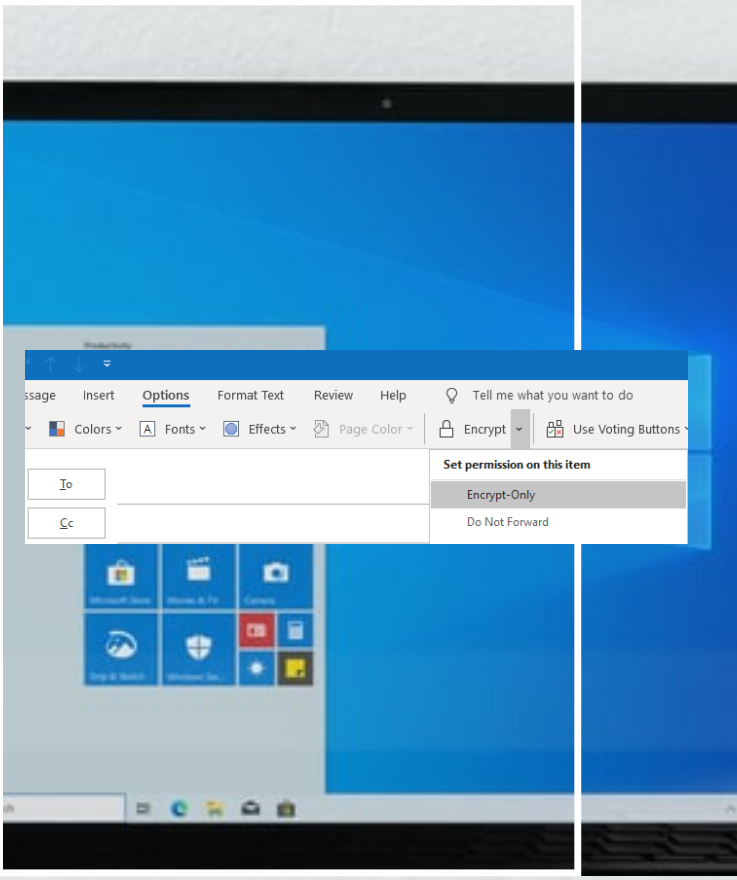
We use multi-factor authentication to access email and other apps

Protecting your RIA from the threat of stolen credentials is crucial. Adding muti-factor authentication (MFA) to all your apps – including Outlook - helps minimize the risk. MFA will always be more secure than even the most complex passwords. You have multiple choices for a second verification process including SMS, voice messages, or the Microsoft Authenticator app.



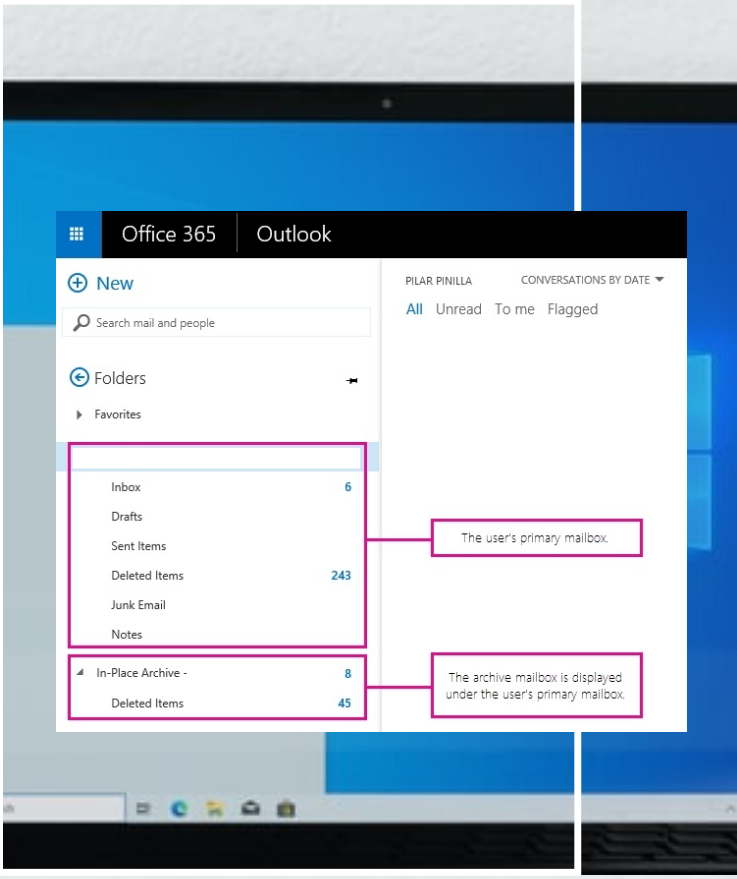
We encrypt emails that include sensitive information

Email encryption is an essential tool for sharing confidential or personal information. It's especially important if you're unsure of the security of the recipient's email server. An encrypted email never leaves Microsoft 365 and the recipient can either access the contents via their own Microsoft 365 account or with the use of a password. You can use encryption to stop messages and attachments from being copied or forwarded.



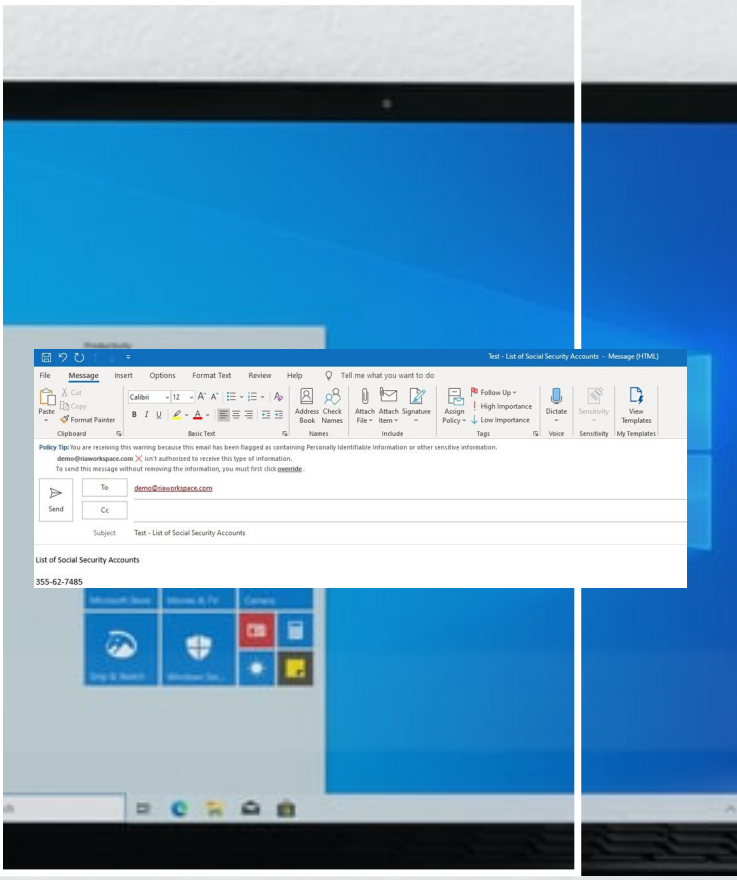
We have email archiving in place

Proper email archiving will keep all your important data in one place with enterprise-level safeguards to protect it. It also gives you easy access from anywhere and eDiscovery features that help you easily find what you're looking for. Archived email data is continuously backed up and supports your compliance and retention requirements.



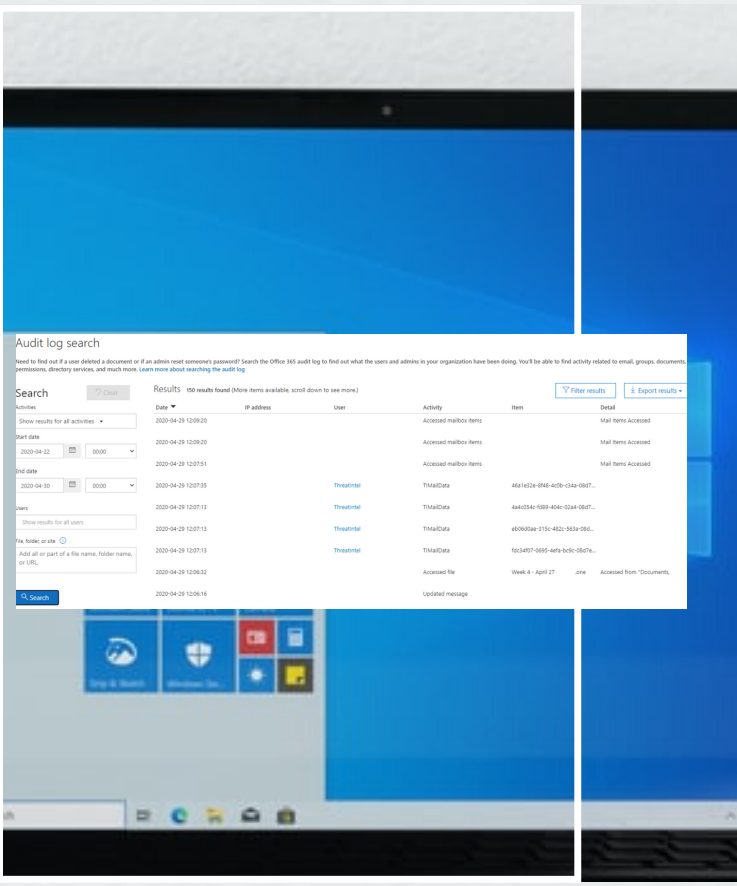
We use advanced data loss tools to prevent sensitive information being sent over email

Advanced data loss prevention (DLP) features help prevent unintentional and intentional sharing of sensitive information like account or social security numbers. Your RIA can establish a DLP policy which outlines your definition of "sensitive information" letting you monitor and safeguard the access and sharing of that information. DLP policies can apply to your entire system and not just your email.



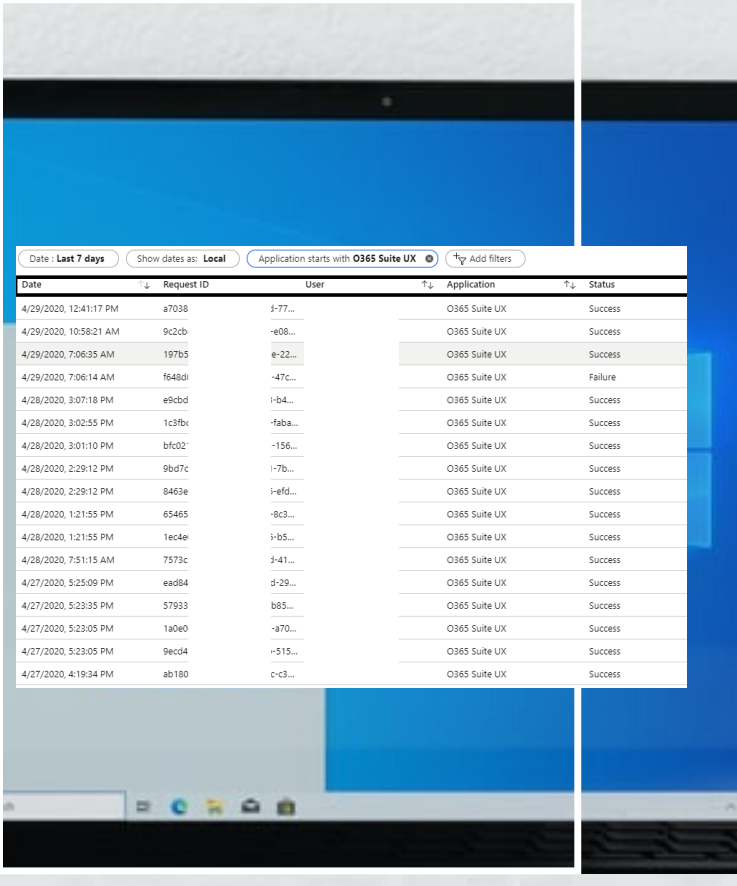
We use email audits to monitor unauthorized use or access

Email auditing gives you control over who accesses a mailbox and what actions they can take. This is especially important when non-owners access a mailbox, included delegate and admin users. You can specify what a non-owner can and can't do and review audit logs to confirm or trace past actions. It's possible to configure your email audit logs to include owners and customize the log retention standards beyond the standard 90 days.



We have configured our advanced threat protection features

Advanced threat protection (ATP) is a pro-active approach to block threats from malware and viruses. Message and attachments are scanned for known malware or warning signs. Questionable emails are isolated and evaluated and only forwarded to the intended inbox if no malicious intent is identified. Your IT department also has insight into the kinds of attacks happening to your RIA so you can focus your priorities.



We secure email access on all devices, including employee-owned devices

Employees access their work email on the same devices they use to view personal email, visit websites, and install personal apps. With proper device management you can confirm that any device or app accessing your data or network is compliant with your security standards. You can also easily manage and revoke access when an employee leaves or a device is lost or stolen.

We provide regular employee safety training

Security threats never stop so neither should your training. It isn't a one-time thing. Use a combination of formalized training, how-to videos, tips and tricks, and always notify employees of new threats and security features. Try to schedule a formal annual or semi-annual training program.

How many did you say "Yes" to?

If you're had 8 out of 8, congratulations!

If not, contact your IT person to implement these features. If they can't, we'd love to help you with it.

If you're ready to work with a highly responsive IT firm that you can trust and understands the unique requirements of your RIA, we would love to hear from you.

Let us show you what fast, friendly, no excuse specialized IT services can do for your RIA.