PREVEIL

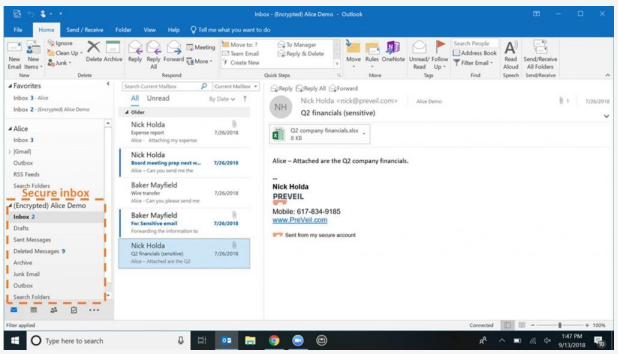
Restoring Trust to everyday business communication

PreVeil's enterprise suite is a secure email and file sharing service that provides a protected communication channel completely insulated from phishing and spoofing attacks. PreVeil's end-to-end encryption architecture (born out of MIT research) also ensures email and file contents stay protected even when passwords are stolen, IT Admin accounts are compromised, and servers are breached. PreVeil is turnkey to deploy and seamlessly integrates with popular mail clients, browsers, and mobile devices - end-users love how easy it is to use.

PreVeil is a secure email and file sharing service that seamlessly protects high risk user groups

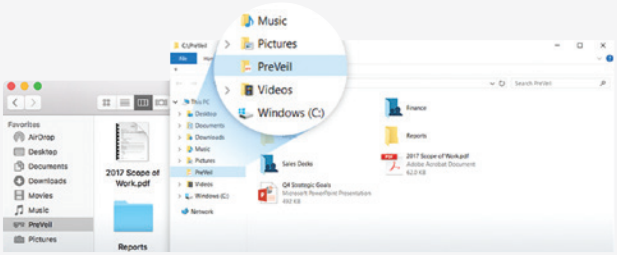
PreVeil Email ("Trusted Mailbox")

Insulates users from phishing / spoofing and keeps emails secure even when passwords are stolen – works seamlessly with Outlook, Mac Mail, iOS, Android



PreVeil Drive

Users can easily store, sync, and share files – both internally and with 3rd parties – while protected with end-to-end encryption.



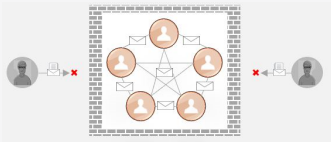
Admin Console

Provision and manage user accounts, access corporate data when required, and monitor logs. Optional integration with Active Directory.

PreVeil security differentiators

Trusted Communities

Insulate users from phishing and spoofing, while enabling collaboration with 3rd parties.



No Passwords

Users don't need to remember passwords. Access is protected by encryption keys on user devices.

Protection for Administrators

Patented Approval Groups™ enable privileged access without granting a single admin keys to the kingdom.

End-to-End Encryption

Protects data even when servers are breached.

...all combined with incredible Ease of Use

PREVEIL

Product features:

PreVeil Email ("Trusted Mailbox") insulates employees from common email attacks and protects email contents even when user credentials are stolen. High risk user groups get a PreVeil Trusted Mailbox that complements their existing (un-trusted) mailbox. Unlike typical email, administrators can restrict 100 percent of external traffic in and out of this Trusted Mailbox. Employees don't need to filter through and attempt to discern whether an incoming email is authentic or malicious – everything that comes in via their Trusted Mailbox can be trusted.

Realizing that most employees don't like the hassle of leaving Outlook to open up a separate email portal (let alone, having to remember yet another password), PreVeil's solution seamlessly integrates with Outlook/ O365. Employees can keep their existing email address with no additional password to remember.

Third parties such as suppliers, customers and partners can also be selectively white-listed into the company's Trusted Community, allowing them to exchange Trusted emails and share files with employees. The result: email collaboration with external parties is just as easy as within your own organization but much more secure.

PreVeil Drive enables end-to-end encrypted file storage and sharing. Users can access files stored on Drive from any of their devices (laptops, mobile phones, tablets). They can also share files with other users with desired access permissions.

Drive is fully integrated into Windows File Explorer and Mac Finder, so encrypted files and folders look and work just like regular ones. It offers the ease of use of popular consumer file sharing services but with advanced enterprise sharing permissions, admin tools, and the protection of end-to-end encryption.

Admin Console enables administrators to easily provision and manage an organization's data. Admins can add and remove users, monitor cryptographic logs, and set or activate organization-wide user and data recovery policies.

Security principles and benefits:

End-to End-Encryption

Attackers can't steal what they can't see. Every document and email is automatically encrypted with a unique key before it leaves a user device and isn't decrypted until it reaches its destination. No one else, not even PreVeil, can read the data because only the sender and recipient have the decryption keys.

Most cloud-based services claim your data is secure because they encrypt data "in transit" and "at rest". In reality, these cloud providers have complete access to your company's data. And so does any hacker who compromises their cloud servers.

Data that's encrypted end-to-end is never decrypted in the cloud. Hence, inevitable attacks on the cloud servers yield only gibberish.

No Passwords

Your account is secured by something much better than passwords – a private encryption key that is only stored on a user's devices. Attackers cannot remotely access a user's account from any other device. Unlike passwords, private keys cannot be guessed by a computer algorithm or stolen from websites.

Approval Groups™

Hijacked or rogue administrators represent a significant threat because they have broad privileges to access an enterprise's information. A single compromised administrator can bring down an entire organization.

PreVeil's Approval Groups™ distribute trust amongst a set of administrators so that no single person can compromise the entire enterprise. Privileged activities are enabled only after receiving cryptographic authorization from a pre-determined set of administrators.