



**April 14, 2015**

**PRESS RELEASE  
FOR IMMEDIATE RELEASE**

**VIR-SEC® Unveils SecureCommunique™:  
An Entirely Private and Secure Application to Communicate**

WASHINGTON, D.C. — Vir-Sec, Inc., a cybersecurity company based out of Clearwater, FL, is unveiling a new private and secure communication application: SecureCommunique™. SecureCommunique™ allows individuals to send emails, documents, files, and chat entirely securely and without fear of external cyber threats.

In March of 2015, CNN reported that Russia may have hacked and monitored the United States State Department’s email system. The event adds to a list of security concerns in the same month, such as that over Hillary Clinton’s private email server, and calls for greater security in private communications has greatly increased.

SecureCommunique™ is the solution that allows users to communicate with complete invisibility and invulnerability to external bad actors. SecureCommunique™ is an application suite used with SecureAccess™, a secure and encrypted USB token unique to each user, therefore exchanges of information are independent of the computer and no communication data is written to the local drive.

**END TO END APPLICATION SECURITY**

A SecureCommunique™ user’s conversation is only visible to their eyes and those with whom they are interacting. Email exchanges and other methods of contact with SecureCommunique™ will be totally removed from the public records of emails. Companies will no longer need to worry about important information exchanges being compromised by hackers because their email networks will only be accessible by internal users.

Companies will no longer have afterthought about a private chat being monitored by nefarious sources. SecureCommunique™ provides the user and the organization with complete privacy and security when communicating via the Internet. Keeping communications secure has never been this easy.

SecureCommunique™ has the look and feel of a standard email application, making it intuitive for customers to use. In the email application, a “memo function” allows users to attach files,

while allowing the option of making the file only available inside SecureCommunique™. Files can also be downloaded inside of SecureCommunique™.

Furthermore, SecureCommunique™ does not use email addresses in the transfer of data. This means that no member of a SecureCommunique group can ever forward data to an outside entity. Most importantly, the absence of email vulnerability means that no one can email any malicious data into the group through phishing techniques, meaning that SecureCommunique™ completely eliminates the threat of phishing or human error.

The chat function is as easy to use as Facebook. First, a SecureCommunique™ user is notified via text or a standard email to “Go Secure” when another user wants to chat in a remote and safe portal. When employing the chat function, a user will see a list of individuals in the group and SecureCommunique™ users will only be able to communicate within this group.

There is nothing complicated to using SecureCommunique™, except for wrapping one’s head around the fact an encrypted USB token is all that is needed to keep their communications completely safe.

SecureCommunique™ is currently in its alpha stage and is FREE with every purchase of SecureAcess™ tokens. Early adopters of the SecureAcess™ “Securing Your Web Portal” program will receive SecureCommunique™ free upon commercial release. Purchasers will also receive a 50% discount on their initial purchase when the beta of SecureCommunique™ is completed and the app is fully launched. Orders and inquiries should be directed to [sales@vir-sec.com](mailto:sales@vir-sec.com).

Users no longer have to forfeit their security when communicating via the Internet.

#### **CONTACT:**

Chris Murphy  
Founder, Chairman & CEO  
Vir-Sec, Inc.  
[management@vir-sec.com](mailto:management@vir-sec.com)

Jared Levine  
Cyber Projects Coordinator  
Vir-Sec, Inc.  
Email: [sales@vir-sec.com](mailto:sales@vir-sec.com)

###