Security Training

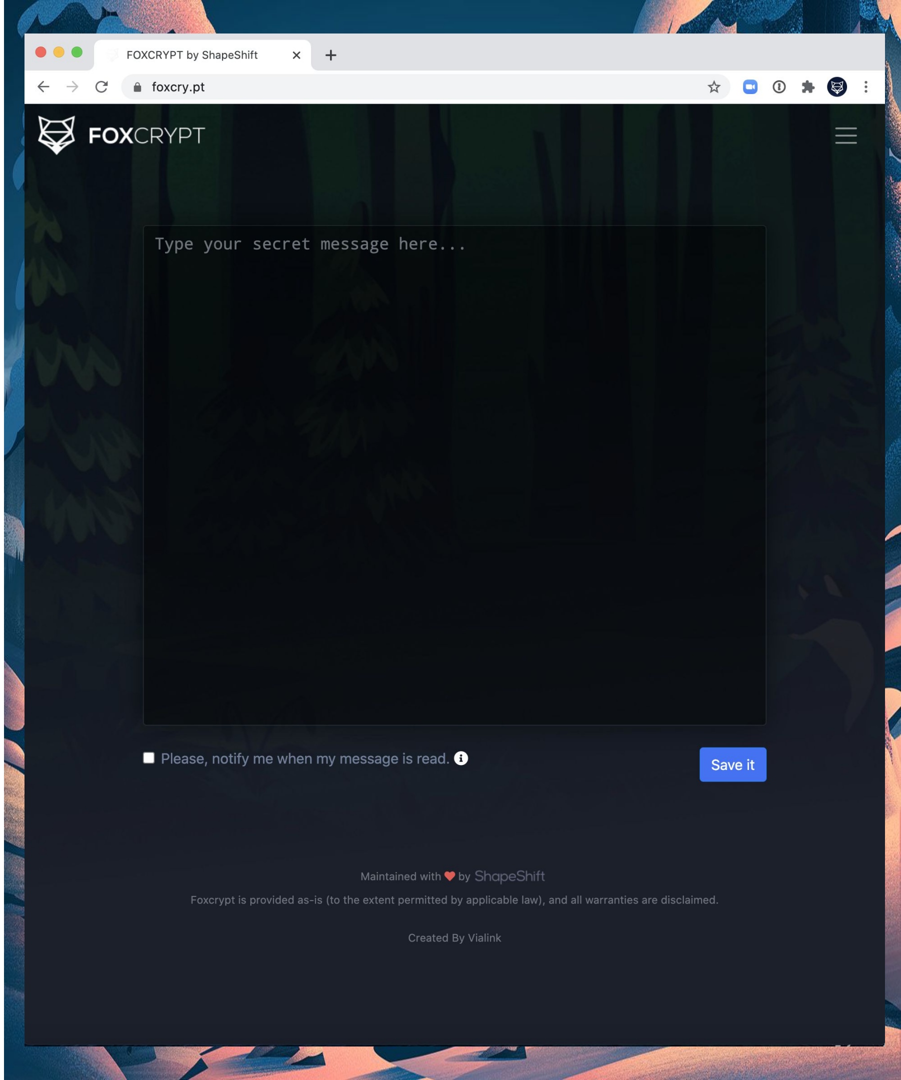
Part 3: Tech Training & Practice

This section will allow you to practice using some of the tools that have been installed in previous training sessions and offer a time to ask questions.

Foxcry.pt

Website to quickly and securely share text with other foxes (https://foxcry.pt)

- Auto-destructs messages after they’re read
- Great way to share API keys, customer PII, and other sensitive data with foxes



Type your secret message here...

□ Please, notify me when my message is read.

Maintained with ❤ by ShapeShift

Foxcrypt is provided as-is (to the extent permitted by applicable law), and all warranties are disclaimed.

Created By Vialink

GPG Practice

GPG is what ShapeShift uses for Encryption.

It has four primary functions:

- Encrypt a message
- Decrypt a message
- Sign a message
- Verify a message

Encryption vs. Digital Signatures

Encryption protects **confidentiality** of data

- It hides information from others

Digital Signatures protect **integrity** and **authenticity** of data

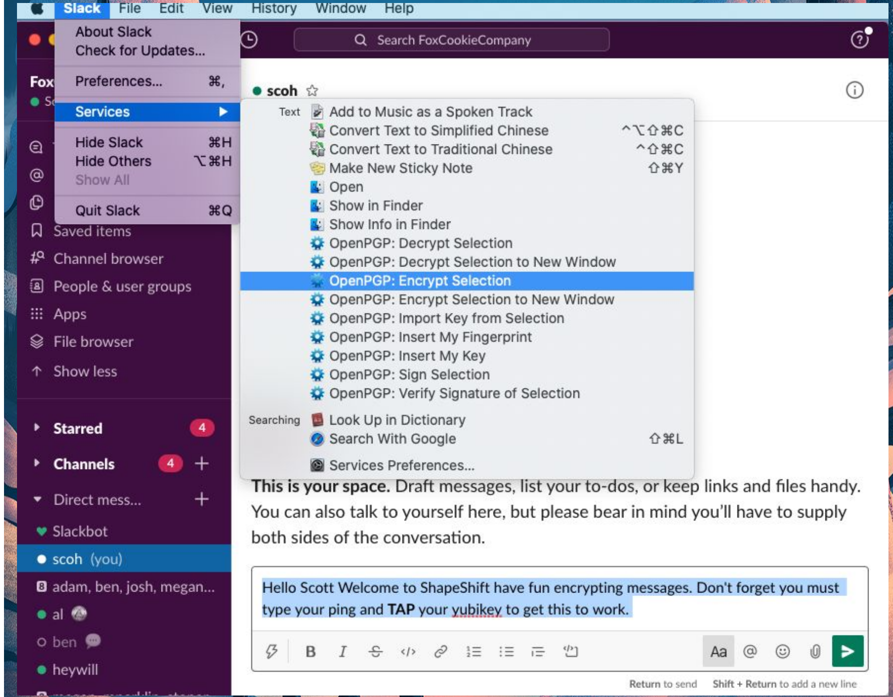
- It shows unauthorized changes
- It allows recipients to know the true author
  - Like a wax seal on an envelope

GPG Practice Encrypt

Encrypt a message (Slack Example):

- Pick your recipient (Slack)
- Type your message in Slack (don’t hit enter)
- Highlight your message
- Slack Menu → Service → OpenPGP: Encrypt Selection

Key Point: The **Services** menu is on every app!



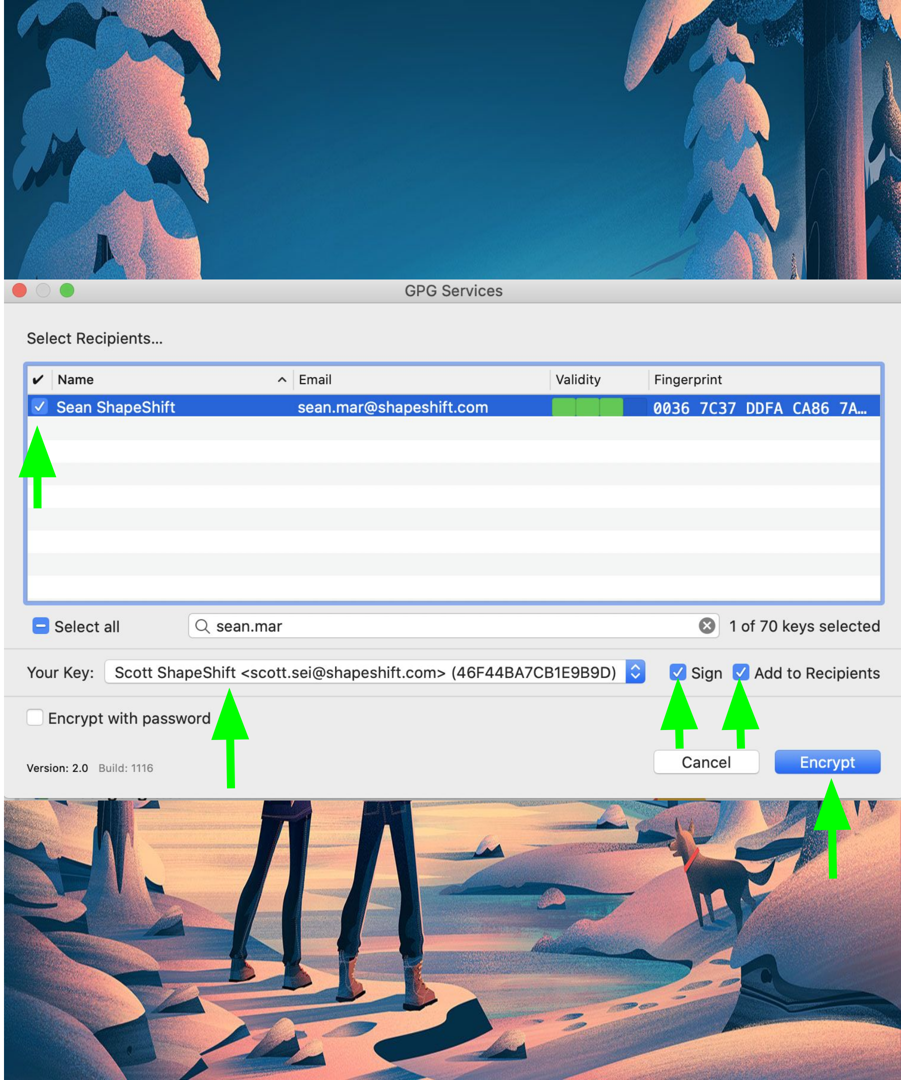
This is your space. Draft messages, list your to-dos, or keep links and files handy. You can also talk to yourself here, but please bear in mind you’ll have to supply both sides of the conversation.

Hello Scott Welcome to ShapeShift have fun encrypting messages. Don't forget you must type your ping and **TAP** your yubikey to get this to work.

GPG Practice Encrypt

Encrypt a message (Slack Example):

- Pick your recipient(s) (GPG)
- Make sure you private key is selected
- Make sure **Sign** is selected
- Make sure **Add to Recipients** is selected
- Press Encrypt



Select Recipients...

✔	Name	Email	Validity	Fingerprint
☑	Sean ShapeShift	sean.mar@shapeshift.com	🟩🟩🟩	0036 7C37 DDFA CA86 7A…

▣ Select all   sean.mar   1 of 70 keys selected

Your Key: Scott ShapeShift <scott.sei@shapeshift.com> (46F44BA7CB1E9B9D)   ☑ Sign   ☑ Add to Recipients

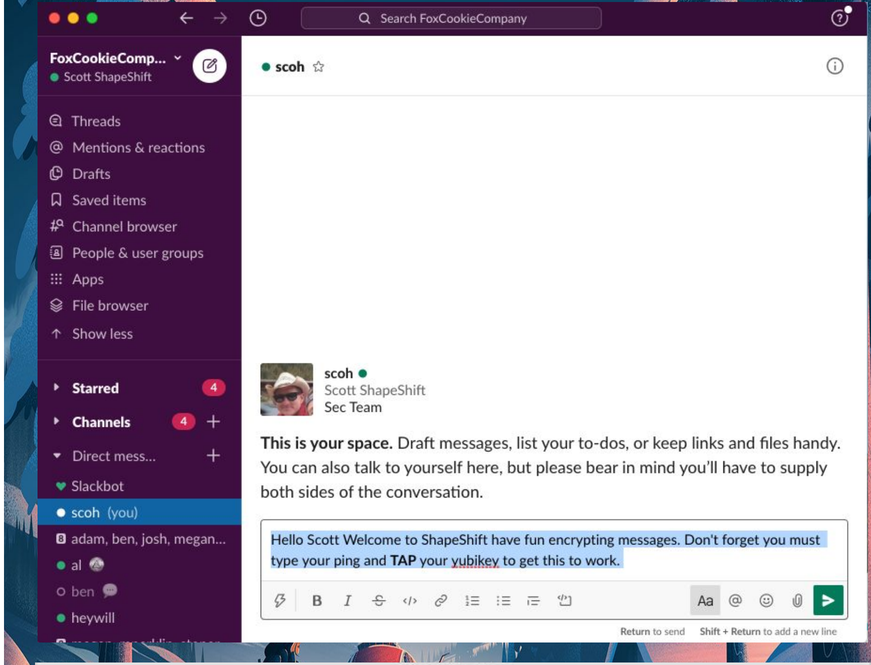
□ Encrypt with password

Version: 2.0 Build: 1116

GPG Practice Encrypt

Encrypt a message (Slack Example):

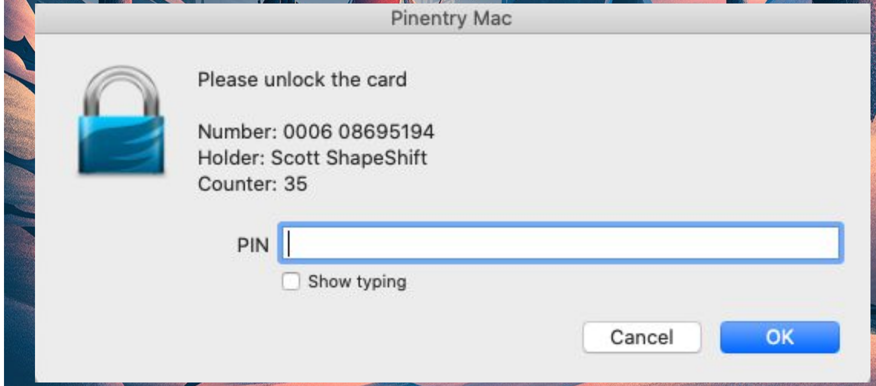
- GPG will prompt you for your 6 digit PIN
- After you enter your PIN (Look at your Yubikey)



scoh
Scott ShapeShift
Sec Team

This is your space. Draft messages, list your to-dos, or keep links and files handy. You can also talk to yourself here, but please bear in mind you'll have to supply both sides of the conversation.

Hello Scott Welcome to ShapeShift have fun encrypting messages. Don't forget you must type your ping and **TAP** your yubikey to get this to work.



Pinentry Mac

Please unlock the card

Number: 0006 08695194
Holder: Scott ShapeShift
Counter: 35

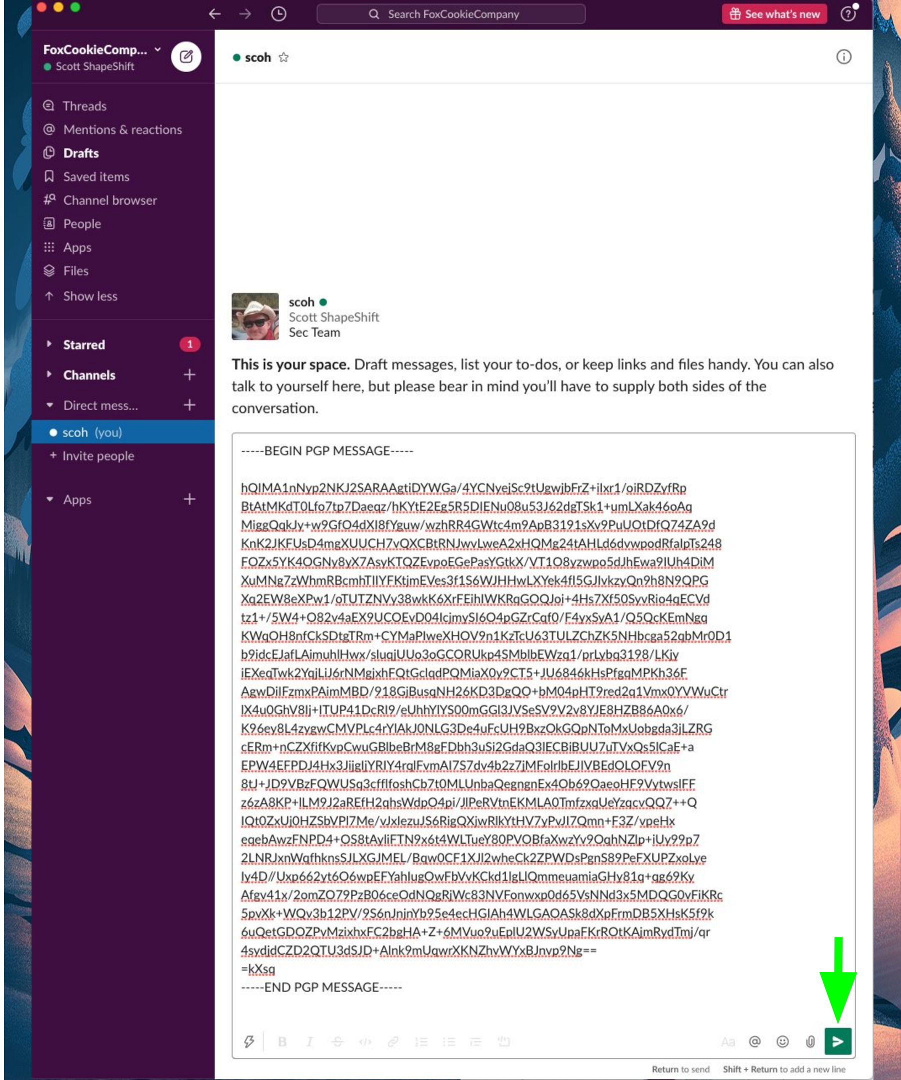
PIN

□ Show typing

GPG Practice Encrypt

Encrypt a message (Slack Example):

- Short Tap your Yubikey to complete the process to see this the encrypted message in slack
- Hit Enter to send!



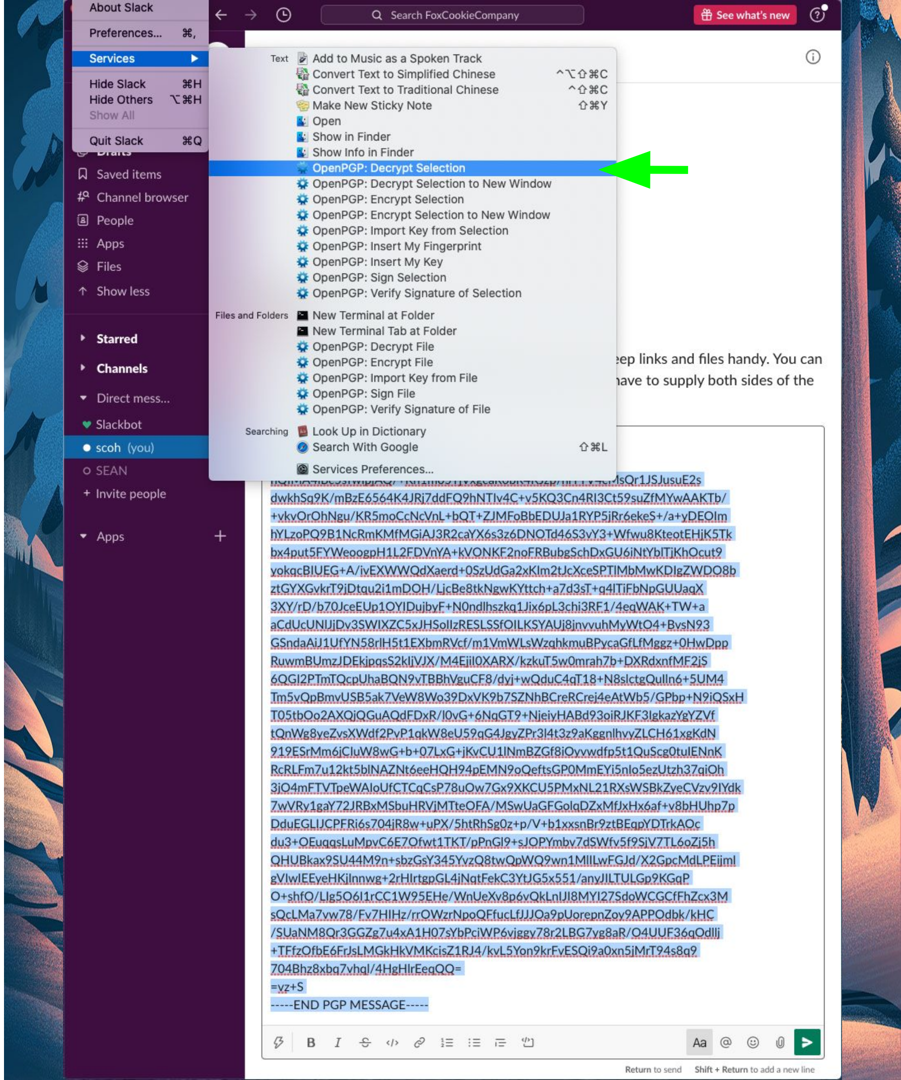
This is your space. Draft messages, list your to-dos, or keep links and files handy. You can also talk to yourself here, but please bear in mind you'll have to supply both sides of the conversation.

```
-----BEGIN PGP MESSAGE-----

hQIMA1nNyp2NKJ2SARAAgtiDYWGa/4YCNyejSc9tUgwjbFrZ+ilxr1/oiRDZyfRp
BtAtMKdT0Lfo7tp7Daeqz/hKYtE2Eg5R5DIENu08u53J62dgTSk1+umLXak46oAq
MiggQqkJy+w9GfO4dXI8fYguw/wzhRR4GWtc4m9ApB3191sXv9PuUOtDfQ74ZA9d
KnK2JKFUsD4mgXUUCH7vQXCBtRNJwvLweA2xHQMg24tAHLd6dvwpodRfalpTs248
FOZx5YK4OGNy8yX7AsyKTQZEvpoEGePasYGtkX/VT1O8yzwpo5dJhEwa9IUh4DiM
XuMNg7zWhmRBcmhTIlYFKtjmEVes3f1S6WJHHwLXYek4fI5GJIvkzyQn9h8N9QPG
Xq2EW8eXPw1/oTUTZNVy38wkK6XrFEihIWKRqGOQJoi+4Hs7Xf50SyvRio4qECVd
tz1+/5W4+O82v4aEX9UCOEvD04IcjmySI6O4pGZrCqf0/F4yxSyA1/Q5QcKEmNgq
KWqOH8nfCkSDtgTRm+CYMaPIweXHOV9n1KzTcU63TULZChZK5NHbcga52qbMr0D1
b9idcEJafLAimuhlHwx/sluqjUUo3oGCORUkp4SMblbEWzq1/prLybq3198/LKjy
iEXeqTwk2YqjLiJ6rNMgjxhFQtGclqdPQMiaX0y9CT5+JU6846kHsPfgqMPKh36F
AgwDiIFzmxPAimMBD/918GjBusqNH26KD3DgQO+bM04pHT9red2q1Vmx0YVWuCtr
lX4u0GhV8Ij+ITUP41DcRI9/eUhhYlYS00mGGl3JVSeSV9V2v8YJE8HZB86A0x6/
K96ey8L4zygwCMVPLc4rYIAkJ0NLG3De4uFcUH9BxzOkGQpNToMxUobgda3jLZRG
cERm+nCZXfifKvpCwuGBlbeBrM8gFDbh3uSi2GdaQ3IECBiBUU7uTVxQs5lCaE+a
EPW4EFPDJ4Hx3JijgljYRIY4rqlFvmAI7S7dv4b2z7jMFolrlbEJIVBEdOLOFV9n
8tJ+JD9VBzFQWUSq3cfflfoshCb7t0MLUnbaQegngnEx4Ob69OaeoHF9VytwslFF
z6zA8KP+lLM9J2aREfH2qhsWdpO4pi/JlPeRVtnEKMLA0TmfzxqUeYzqcvQQ7++Q
IQt0ZxUj0HZSbVPl7Me/vJxlezuJS6RigQXjwRlkYtHV7yPvJI7Qmn+F3Z/vpeHx
eqebAwzFNPD4+OS8tAyliFTN9x6t4WLTueY80PVOBfaXwzYv9OqhNZlp+iUy99p7
2LNRJxnWqfhknsSJLXGJMEL/Bqw0CF1XJl2wheCk2ZPWDsPgnS89PeFXUPZxoLye
Iy4D//Uxp662yt6O6wpEFYahIugOwFbVvKCkd1IgLIQmmeuamiaGHy81q+qg69Ky
Afgv41x/2omZO79PzB06ceOdNQgRjWc83NVFonwxp0d65VsNNd3x5MDQG0vFiKRc
5pvXk+WQv3b12PV/9S6nJnjnYb95e4ecHGIAh4WLGAOASk8dXpFrmDB5XHsK5f9k
6uQetGDOZPvMzixhxFC2bgHA+Z+6MVuo9uEplU2WSyUpaFKrROtKAjmRydTmj/qr
4sydjdCZD2QTU3dSJD+AInk9mUqwrXKNZhvWYxBJnvp9Ng==
=kXsq
-----END PGP MESSAGE-----
```

GPG Practice Decrypt

Decrypt a message (Slack Example):

- Highlight the messages
- Slack Menu → Service → OpenPGP: Decrypt Selection

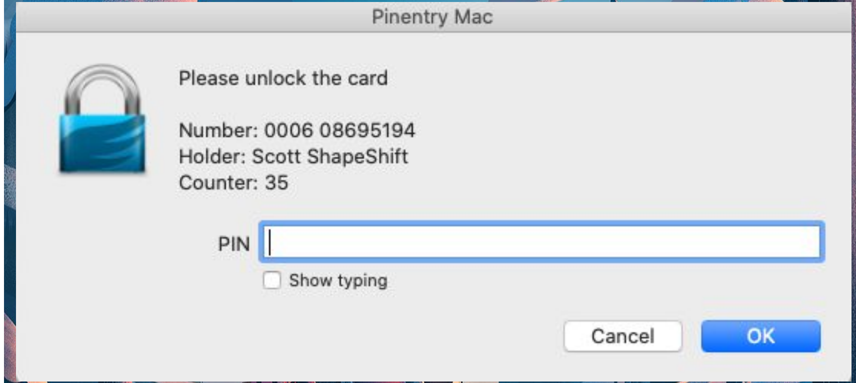


MsQr1JSJusuE2s
dwkhSq9K/mBzE6564K4JRj7ddFQ9hNTIv4C+v5KQ3Cn4RI3Ct59suZfMYwAAKTb/
+vkvOrOhNgu/KR5moCcNcVnL+bQT+ZJMFoBbEDUJa1RYP5jRr6ekeS+/a+yDEOIm
hYLzoPQ9B1NcRmKMfMGiAJ3R2caYX6s3z6DNOTd46S3vY3+Wfwu8KteotEHjK5Tk
bx4put5FYWeoogpH1L2FDVnYA+kVONKF2noFRBubgSchDxGU6iNtYblTjKhOcut9
yokqcBIUEG+A/ivEXWWQdXaerd+0SzUdGa2xKIm2tJcXceSPTIMbMwKDIgZWDO8b
ztGYXGvkrT9jDtqu2i1mDOH/LjcBe8tkNgwKYttch+a7d3sT+q4lTiFbNpGUUaqX
3XY/rD/b70JceEUp1OYIDujbyF+N0ndlhszkq1Jix6pL3chi3RF1/4eqWAK+TW+a
aCdUcUNIJjDv3SWIXZC5xJHSoIlzRESLSSfOILKSYAUj8jnvvuhMyWtO4+BvsN93
GSndaAiJ1UfYN58rlH5t1EXbmRVcf/m1VmWLsWzqhkmuBPycaGfLfMggz+0HwDpp
RuwmBUmzJDEkjpqsS2kIjVJX/M4Ejil0XARX/kzkuT5w0mrah7b+DXRdxnfMF2jS
6QGI2PTmTQcpUhaBQN9vTBBhVguCF8/dyj+wQduC4qT18+N8slctgQuIln6+5UM4
Tm5vQpBmvUSB5ak7VeW8Wo39DxVK9b7SZNhBCreRCrej4eAtWb5/GPbp+N9iQSxH
T05tbOo2AXQjQGuAQdFDxR/l0vG+6NqGT9+NjeiyHABd93oiRJKF3IgkazYgYZVf
tQnWg8yeZvsXWdf2PvP1qkW8eU59qG4JgyZPr3l4t3z9aKggnlhvyZLCH61xgKdN
919ESrMm6jCIuW8wG+b+07LxG+jKvCU1INmBZGf8iOyvwdfp5t1QuScg0tuIENnK
RcRLFm7u12kt5blNAZNt6eeHQH94pEMN9oQeftsGP0MmEYi5nlo5ezUtzh37qiOh
3jO4mFTVTpeWAIoUfCTCqCsP78uOw7Gx9XKCU5PMxNL21RXsWSBkZyeCVzv9IYdk
7wVRy1gaY72JRBxMSbuHRVjMTteOFA/MSwUaGFGolqDZxMfJxHx6af+v8bHUhp7p
DduEGLIJCPFRi6s704jR8w+uPX/5htRhSg0z+p/V+b1xxsnBr9ztBEqpYDTrkAOc
du3+OEuqqsLuMpvC6E7Ofwt1TKT/pPnGl9+sJOPYmbv7dSWfv5f9SjV7TL6oZj5h
QHUBkax9SU44M9n+sbzGsY345YvzQ8twQpWQ9wn1MIILwFGJd/X2GpcMdLPEijml
gVIwIEEyeHKjlnnwg+2rHIrtgpGL4jNqtFekC3YtJG5x551/anyJILTULGp9KGqP
O+shfO/LIg5O6I1rCC1W95EHe/WnUeXv8p6vQkLnIJI8MYI27SdoWCGCfFhZcx3M
sQcLMa7vw78/Fv7HIHz/rrOWzrNpoQFfucLfJJJOa9pUorepnZoy9APPOdbk/kHC
/SUaNM8Qr3GGZg7u4xA1H07sYbPciWP6vjggy78r2LBG7yg8aR/O4UUF36qOdllj
+TFfzOfbE6FrJsLMGkHkVMKcisZ1RJ4/kvL5Yon9krFvESQi9a0xn5jMrT94s8q9
704Bhz8xbq7vhql/4HgHlrEeqQQ=
=vz+S
-----END PGP MESSAGE-----

GPG Practice Decrypt

Decrypt a message (Slack Example):

- GPG will prompt you for your 6 digits PIN
- After you enter your PIN (Look at your Yubikey)



Pinentry Mac

Please unlock the card

Number: 0006 08695194
Holder: Scott ShapeShift
Counter: 35

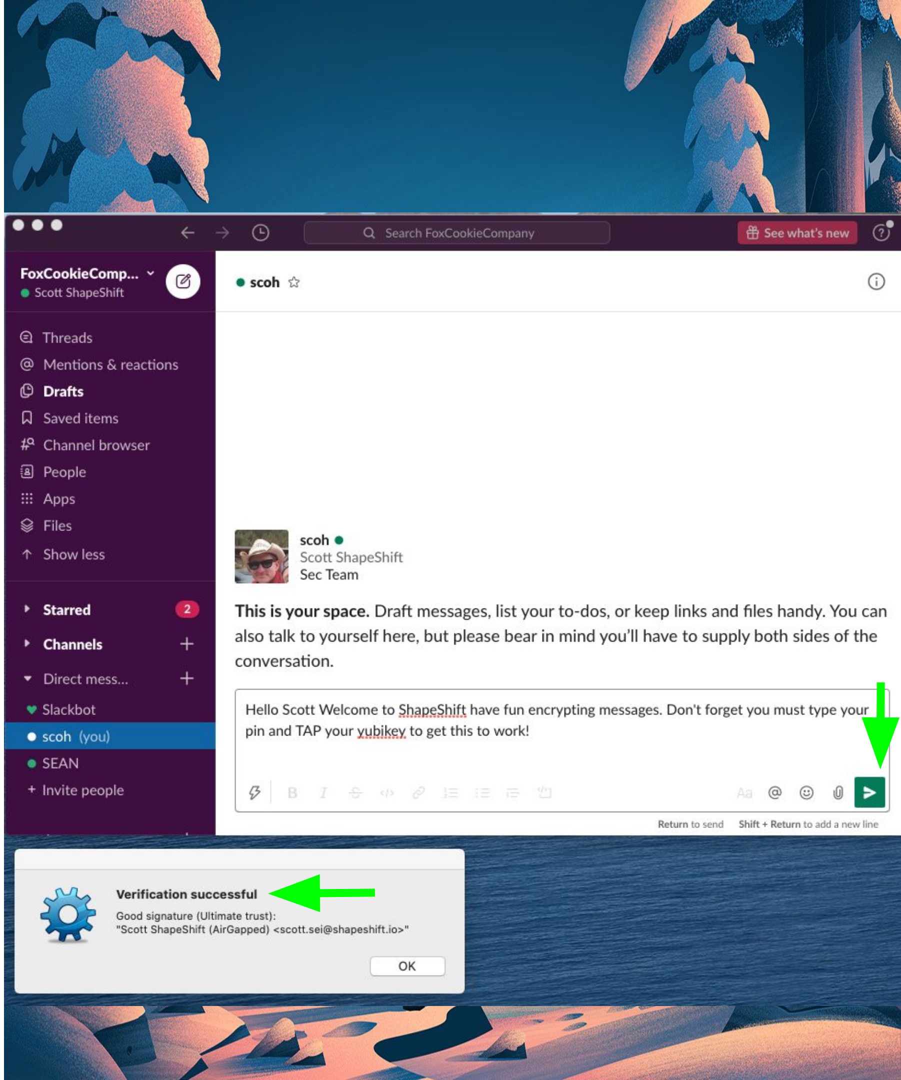
PIN

□ Show typing

GPG Practice Decrypt

Decrypt a message (Slack Example):

- Short Tap your Yubikey to complete the process to see this the decrypted message in Slack
- A verification popup from GPG will show success



This is your space. Draft messages, list your to-dos, or keep links and files handy. You can also talk to yourself here, but please bear in mind you'll have to supply both sides of the conversation.

Hello Scott Welcome to ShapeShift have fun encrypting messages. Don't forget you must type your pin and TAP your yubikey to get this to work!

Verification successful

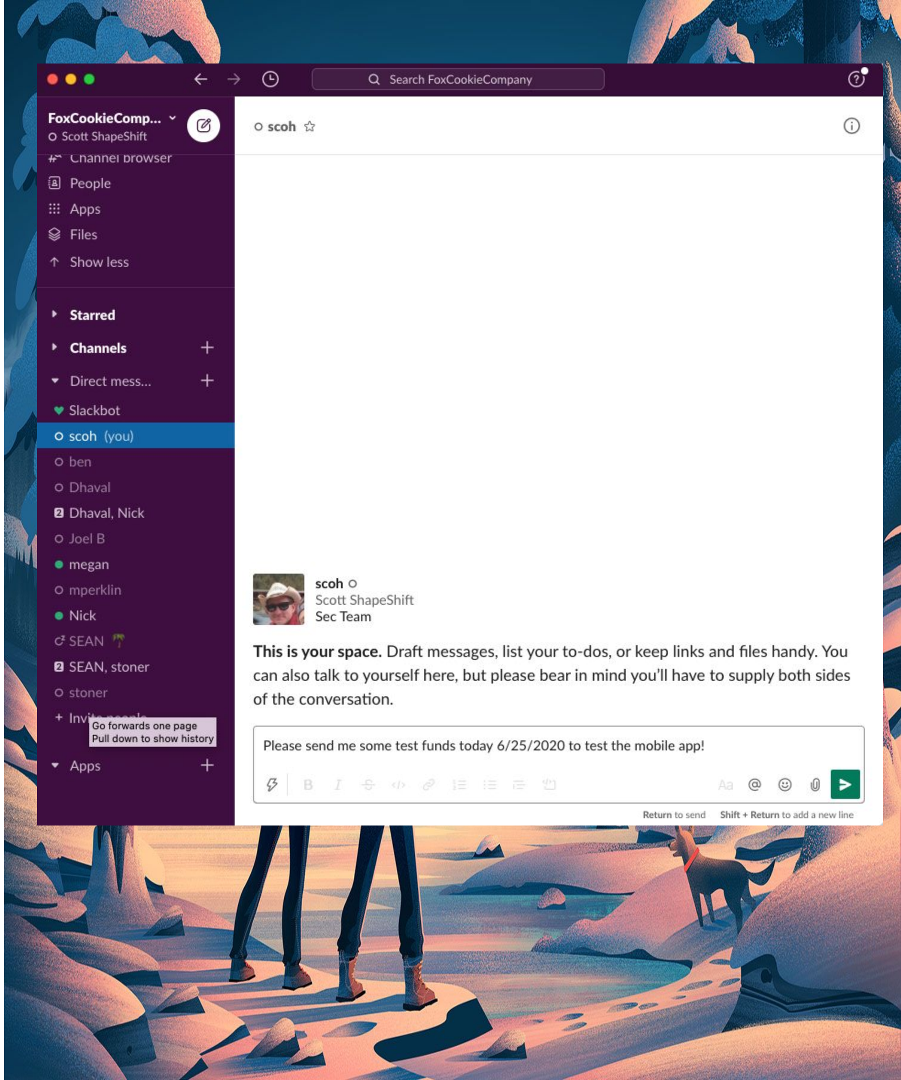
Good signature (Ultimate trust):
"Scott ShapeShift (AirGapped) <scott.sei@shapeshift.io>"

Questions

GPG Practice Signing

Sign a message (Slack Example):

- Type your message in slack
- Don’t hit enter



scoh
Scott ShapeShift
Sec Team

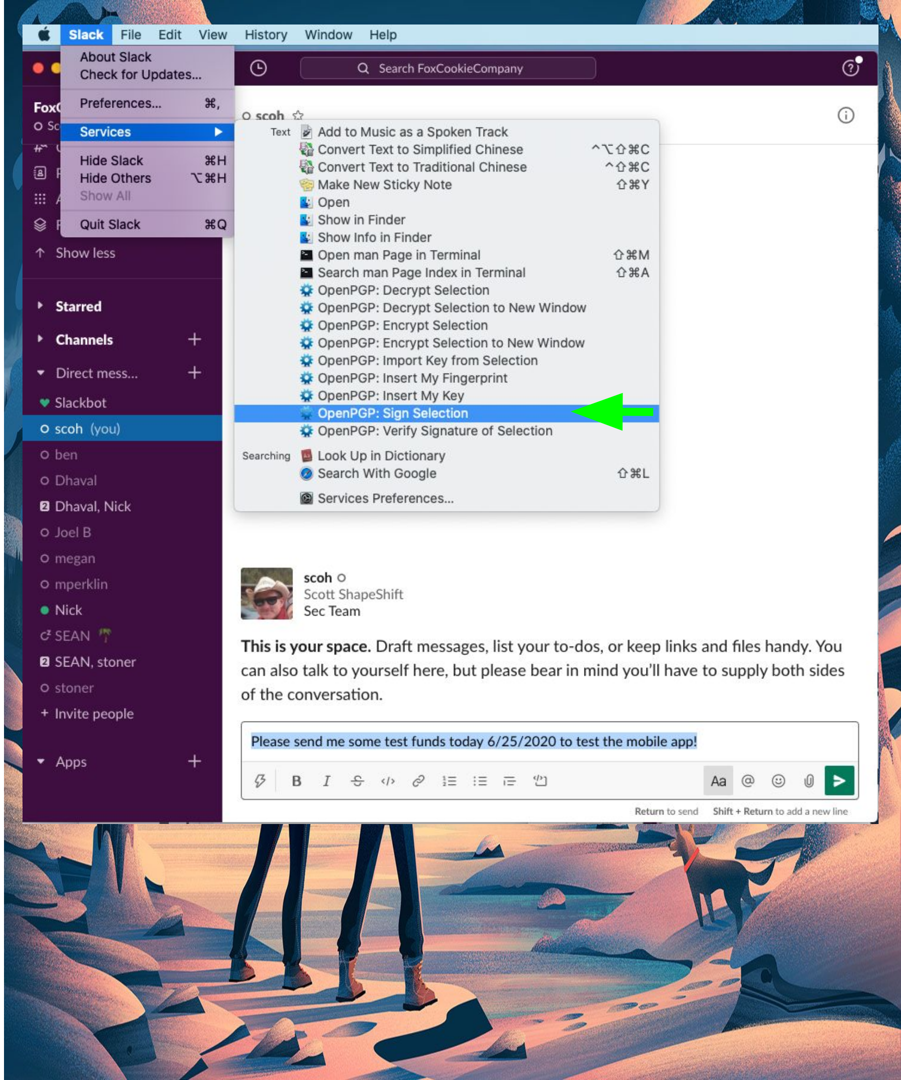
This is your space. Draft messages, list your to-dos, or keep links and files handy. You can also talk to yourself here, but please bear in mind you’ll have to supply both sides of the conversation.

Please send me some test funds today 6/25/2020 to test the mobile app!

GPG Practice Signing (continued)

Sign a message (Slack Example):

- Highlight you message
- Slack Menu → Service → OpenPGP: Sign Selection



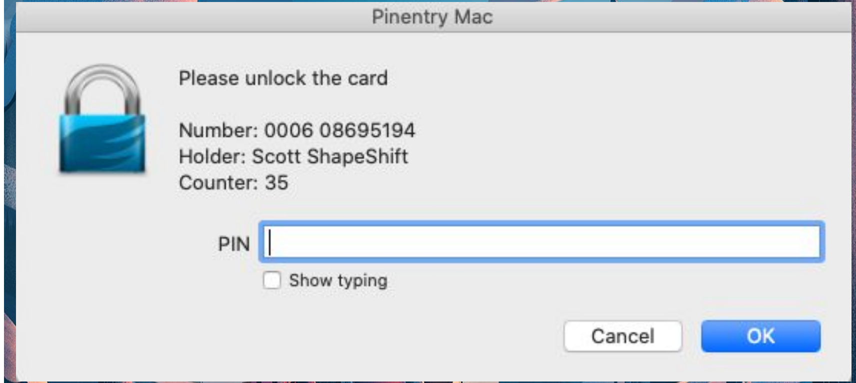
This is your space. Draft messages, list your to-dos, or keep links and files handy. You can also talk to yourself here, but please bear in mind you'll have to supply both sides of the conversation.

Please send me some test funds today 6/25/2020 to test the mobile app!

GPG Practice Signing (continued)

Sign a message (Slack Example):

- GPG will prompt you for your 6 digit PIN
- After you enter your PIN (Look at your Yubikey)



Please unlock the card

Number: 0006 08695194
Holder: Scott ShapeShift
Counter: 35

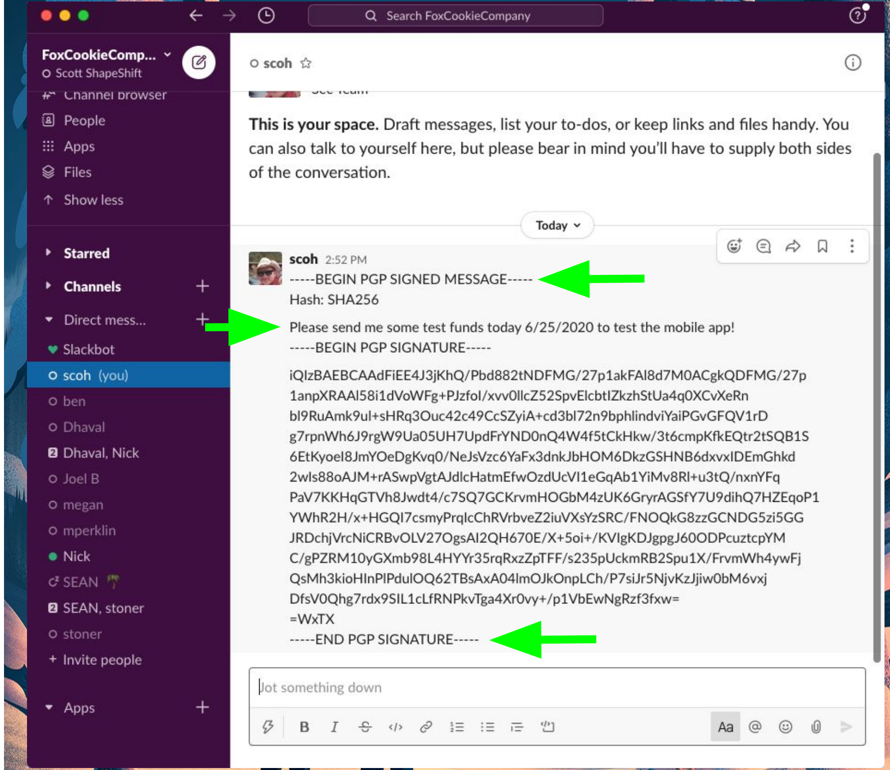
PIN

□ Show typing

GPG Practice Signing (continued)

Sign a message (Slack Example):

- Notice you message is still there but it is now wrapped with your GPG signature
- Press enter to send



This is your space. Draft messages, list your to-dos, or keep links and files handy. You can also talk to yourself here, but please bear in mind you'll have to supply both sides of the conversation.

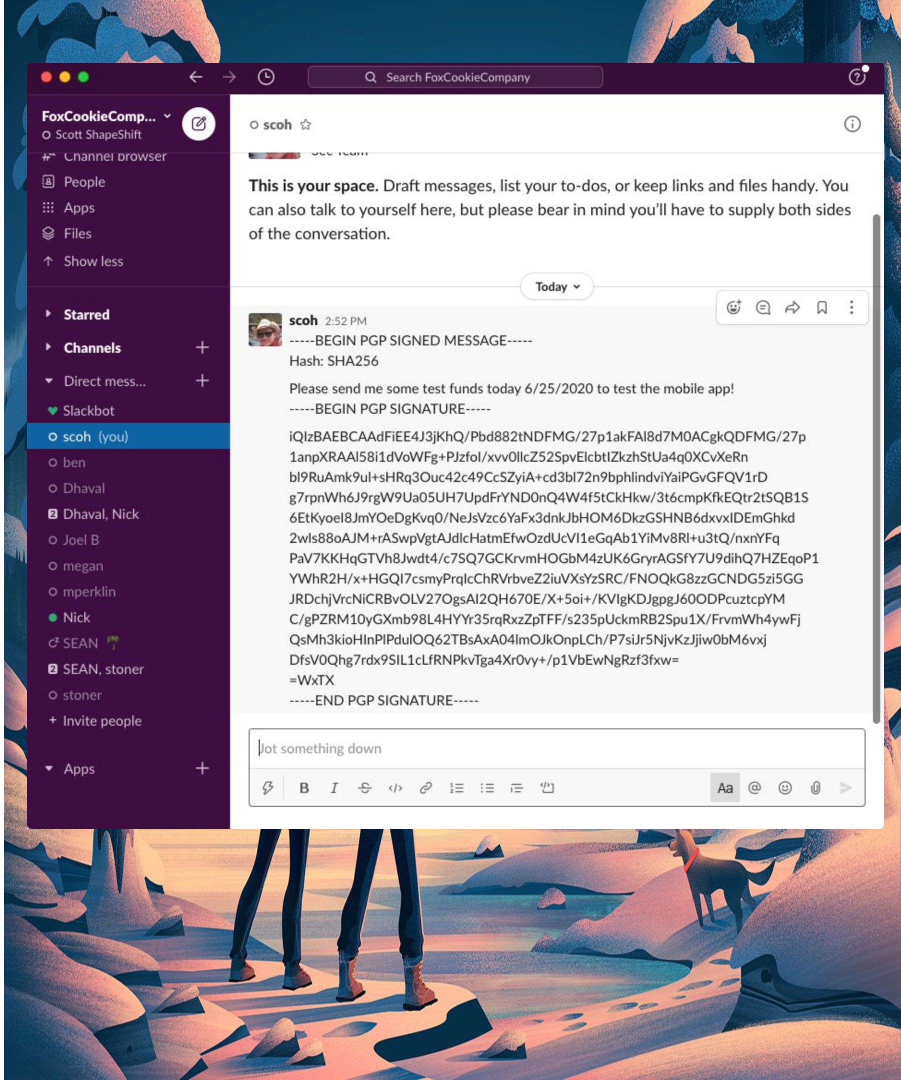
scoh 2:52 PM

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Please send me some test funds today 6/25/2020 to test the mobile app!
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEE4J3jKhQ/Pbd882tNDFMG/27p1akFAl8d7M0ACgkQDFMG/27p
1anpXRAAl58i1dVoWFg+PJzfol/xvv0llcZ52SpvElcbtIZkzhStUa4q0XCvXeRn
bl9RuAmk9ul+sHRq3Ouc42c49CcSZyiA+cd3bl72n9bphlindviYaiPGvGFQV1rD
g7rpnWh6J9rgW9Ua05UH7UpdFrYND0nQ4W4f5tCkHkw/3t6cmpKfkEQtr2tSQB1S
6EtKyoel8JmYOeDgKvq0/NeJsVzc6YaFx3dnkJbHOM6DkzGSHNB6dxvxIDEmGhkd
2wIs88oAJM+rASwpVgtAJdlcHatmEfwOzdUcVI1eGqAb1YiMv8Rl+u3tQ/nxnYFq
PaV7KKHqGTVh8Jwdt4/c7SQ7GCKrvmHOGbM4zUK6GryrAGSfY7U9dihQ7HZEqoP1
YWhR2H/x+HGQI7csmyPrqlcChRVrbveZ2iuVXsYzSRC/FNOQkG8zzGCNDG5zi5GG
JRDchjVrcNiCRBvOLV27OgsAI2QH670E/X+5oi+/KVIgKDJgpgJ60ODPcuztcpYM
C/gPZRM10yGXmb98L4HYYr35rqRxzZpTFF/s235pUckmRB2Spu1X/FrvmWh4ywFj
QsMh3kioHInPlPdulOQ62TBsAxA04lmOJkOnpLCh/P7siJr5NjvKzJjiw0bM6vxj
DfsV0Qhg7rdx9SIL1cLfRNPkvTga4Xr0vy+/p1VbEwNgRzf3fxw=
=WxTX
-----END PGP SIGNATURE-----
```

GPG Practice Verification

Verify a message (Slack Example):

- You will probably see signed message in Slack.
- There is a Slack/GPG bug that causes verification to fail in Slack
- There's a workaround



This is your space. Draft messages, list your to-dos, or keep links and files handy. You can also talk to yourself here, but please bear in mind you'll have to supply both sides of the conversation.

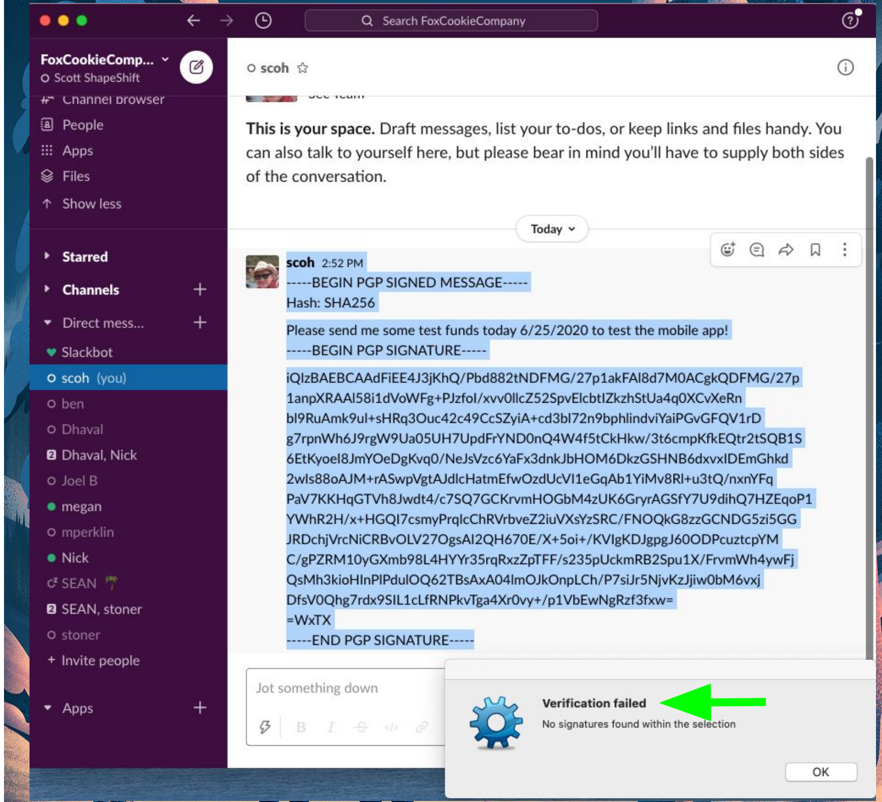
scoh 2:52 PM

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Please send me some test funds today 6/25/2020 to test the mobile app!
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEE4J3jKhQ/Pbd882tNDFMG/27p1akFAl8d7M0ACgkQDFMG/27p
1anpXRAAl58i1dVoWFg+PJzfoI/xvv0llcZ52SpvElcbtIZkzhStUa4q0XCvXeRn
bl9RuAmk9ul+sHRq3Ouc42c49CcSZyiA+cd3bl72n9bphlindviYaiPGvGFQV1rD
g7rpnWh6J9rgW9Ua05UH7UpdFrYND0nQ4W4f5tCkHkw/3t6cmpKfkEQtr2tSQB1S
6EtKyoeI8JmYOeDgKvq0/NeJsVzc6YaFx3dnkJbHOM6DkzGSHNB6dxvxIDEmGhkd
2wIs88oAJM+rASwpVgtAJdlcHatmEfwOzdUcVI1eGqAb1YiMv8Rl+u3tQ/nxnYFq
PaV7KKHqGTVh8Jwdt4/c7SQ7GCKrvmHOGbM4zUK6GryrAGSfY7U9dihQ7HZEqoP1
YWhR2H/x+HGQI7csmyPrqlcChRVrbveZ2iuVXsYzSRC/FNOQkG8zzGCNDG5zi5GG
JRDchjVrcNiCRBvOLV27OgsAI2QH670E/X+5oi+/KVIgKDJgpgJ60ODPcuztcpYM
C/gPZRM10yGXmb98L4HYYr35rqRxzZpTFF/s235pUckmRB2Spu1X/FrvmWh4ywFj
QsMh3kioHInPlPdulOQ62TBsAxA04lmOJkOnpLCh/P7siJr5NjvKzJjiw0bM6vxj
DfsV0Qhg7rdx9SIL1cLfRNPkvTga4Xr0vy+/p1VbEwNgRzf3fxw=
=WxTX
-----END PGP SIGNATURE-----
```

GPG Practice Verification Slack Bug

Verify a message (Slack Example):

- When trying to verify GPG signed message directly in slack it will always error
- Notice the Verification failed message



This is your space. Draft messages, list your to-dos, or keep links and files handy. You can also talk to yourself here, but please bear in mind you'll have to supply both sides of the conversation.

scoh 2:52 PM

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Please send me some test funds today 6/25/2020 to test the mobile app!
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEE4J3jKhQ/Pbd882tNDFMG/27p1akFAl8d7M0ACgkQDFMG/27p
1anpXRAAl58i1dVoWFg+PJzfol/xvv0llcZ52SpvElcbtlZkzhStUa4q0XCvXeRn
bl9RuAmk9ul+sHRq3Ouc42c49CcSZyiA+cd3bl72n9bphlindviYaiPGvGFQV1rD
g7rpnWh6J9rgW9Ua05UH7UpdFrYND0nQ4W4f5tCkHkw/3t6cmpKfkEQtr2tSQB1S
6EtKyoel8JmYOeDgKvq0/NeJsVzc6YaFx3dnkJbHOM6DkzGSHNB6dxvxIDEmGhkd
2wIs88oAJM+rASwpVgtAJdlcHatmEfwOzdUcVI1eGqAb1YiMv8Rl+u3tQ/nxnYFq
PaV7KKHqGTVh8Jwdt4/c7SQ7GCKrvmHOGbM4zUK6GryrAGSfY7U9dihQ7HZEqoP1
YWhR2H/x+HGQI7csmyPrqlcChRVrbveZ2iuVXsYzSRC/FNOQkG8zzGCNDG5zi5GG
JRDchjVrcNiCRBvOLV27OgsAI2QH670E/X+5oi+/KVIgKDJgpgJ60ODPcuztcpYM
C/gPZRM10yGXmb98L4HYYr35rqRxzZpTFF/s235pUckmRB2Spu1X/FrvmWh4ywFj
QsMh3kioHInPlPdulOQ62TBsAxA04lmOJkOnpLCh/P7siJr5NjvKzJjiw0bM6vxj
DfsV0Qhg7rdx9SIL1cLfRNPkvTga4Xr0vy+/p1VbEwNgRzf3fxw=
=WxTX
-----END PGP SIGNATURE-----
```

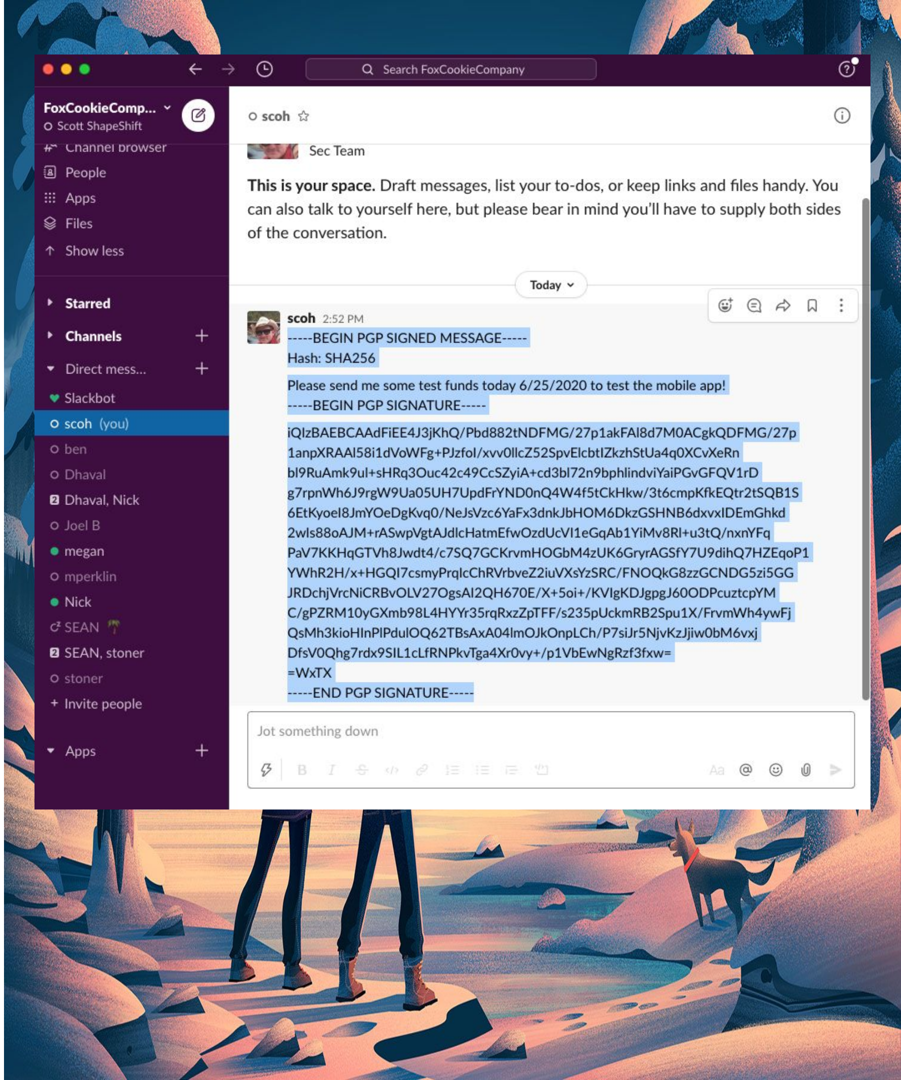
Verification failed

No signatures found within the selection

GPG Practice Verification (continued)

Verify a message (Slack/TextEdit Example):

- Highlight the slack message.
- Make sure you get all the text starting at -----BEGIN PGP SIGNED MESSAGE-----
- Copy the message



This is your space. Draft messages, list your to-dos, or keep links and files handy. You can also talk to yourself here, but please bear in mind you'll have to supply both sides of the conversation.

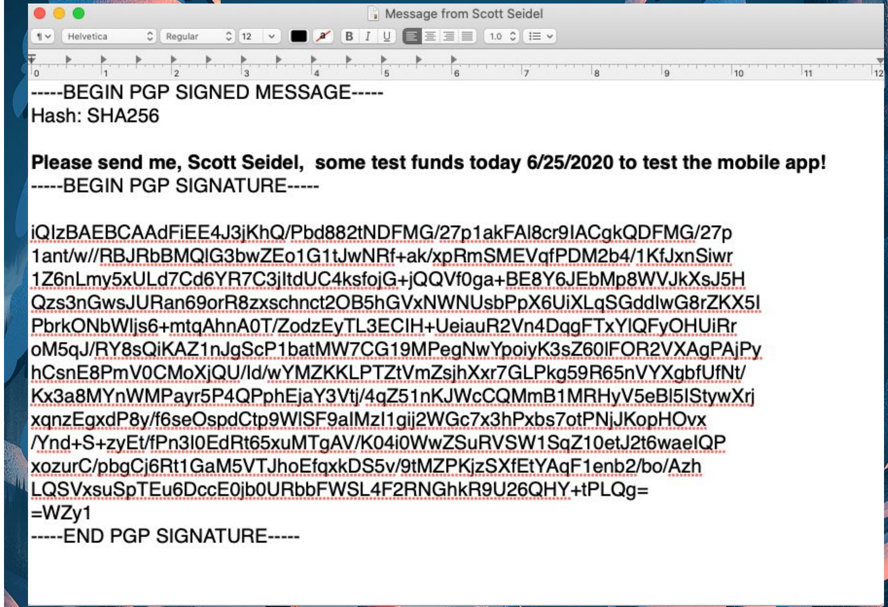
scoh 2:52 PM

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Please send me some test funds today 6/25/2020 to test the mobile app!
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEE4J3jKhQ/Pbd882tNDFMG/27p1akFAl8d7M0ACgkQDFMG/27p
1anpXRAAl58i1dVoWFg+PJzfol/xvv0llcZ52SpvElcbtIZkzhStUa4q0XCvXeRn
bl9RuAmk9ul+sHRq3Ouc42c49CcSZyiA+cd3bl72n9bphlindviYaiPGvGFQV1rD
g7rpnWh6J9rgW9Ua05UH7UpdFrYND0nQ4W4f5tCkHkw/3t6cmpKfkEQtr2tSQB1S
6EtKyoeI8JmYOeDgKvq0/NeJsVzc6YaFx3dnkJbHOM6DkzGSHNB6dxvxIDEmGhkd
2wls88oAJM+rASwpVgtAJdlcHatmEfwOzdUcVI1eGqAb1YiMv8Rl+u3tQ/nxnYFq
PaV7KKHqGTVh8Jwdt4/c7SQ7GCKrvmHOGbM4zUK6GryrAGSfY7U9dihQ7HZEqoP1
YWhR2H/x+HGQI7csmyPrqlcChRVrbveZ2iuVXsYzSRC/FNOQkG8zzGCNDG5zi5GG
JRDchjVrcNiCRBvOLV27OgsAI2QH670E/X+5oi+/KVIgKDJgpgJ60ODPcuztcpYM
C/gPZRM10yGXmb98L4HYYr35rqRxzZpTFF/s235pUckmRB2Spu1X/FrvmWh4ywFj
QsMh3kioHInPlPdulOQ62TBsAxA04lmOJkOnpLCh/P7siJr5NjvKzJjiw0bM6vxj
DfsV0Qhg7rdx9SIL1cLfRNPkvTga4Xr0vy+/p1VbEwNgRzf3fxw=
=WxTX
-----END PGP SIGNATURE-----
```

GPG Practice Verification (continued)

Verify a message (Slack/TextEdit Example):

- Paste the text into an text editor. (TextEdit)

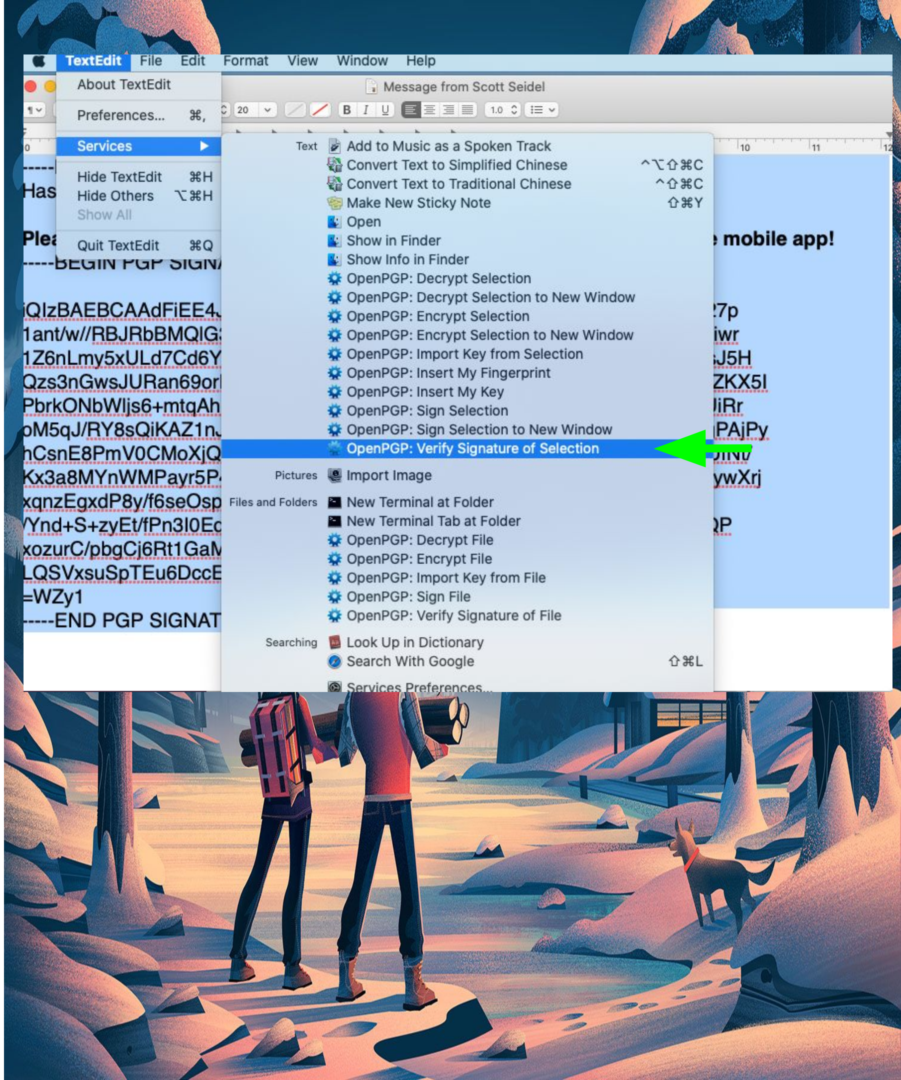


```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Please send me, Scott Seidel,  some test funds today 6/25/2020 to test the mobile app!
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEE4J3jKhQ/Pbd882tNDFMG/27p1akFAl8cr9IACgkQDFMG/27p
1ant/w//RBJRbBMQlG3bwZEo1G1tJwNRf+ak/xpRmSMEVqfPDM2b4/1KfJxnSiwr
1Z6nLmy5xULd7Cd6YR7C3jltdUC4ksfojG+jQQVf0ga+BE8Y6JEbMp8WVJkXsJ5H
Qzs3nGwsJURan69orR8zxschnct2OB5hGVxNWNUsbPpX6UiXLqSGddlwG8rZKX5l
PbrkONbWljs6+mtqAhnA0T/ZodzEyTL3ECIH+UeiauR2Vn4DqgFTxYlQFyOHUiRr
oM5qJ/RY8sQiKAZ1nJgScP1batMW7CG19MPegNwYpoiyK3sZ60lFOR2VXAgPAjPy
hCsnE8PmV0CMoXjQU/Id/wYMZKKLPTZtVmZsjhXxr7GLPkg59R65nVYXgbfUfNt/
Kx3a8MYnWMPayr5P4QPphEjaY3Vtj/4qZ51nKJWcCQMmB1MRHyV5eBl5lStywXrj
xqnzEgxdP8y/f6seOspdCtp9WlSF9aIMzI1gij2WGc7x3hPxbs7otPNjJKopHOvx
/Ynd+S+zyEt/fPn3I0EdRt65xuMTgAV/K04i0WwZSuRVSW1SqZ10etJ2t6waeIQP
xozurC/pbgCj6Rt1GaM5VTJhoEfqxkDS5v/9tMZPKjzSXfEtYAqF1enb2/bo/Azh
LQSVxsuSpTEu6DccE0jb0URbbFWSL4F2RNGhkR9U26QHY+tPLQg=
=WZy1
-----END PGP SIGNATURE-----
```

GPG Practice Verification (continued)

Verify a message (Slack/TextEdit Example):

- Highlight the messages
- Slack Menu → Service → OpenPGP: Verify Signature of Selection

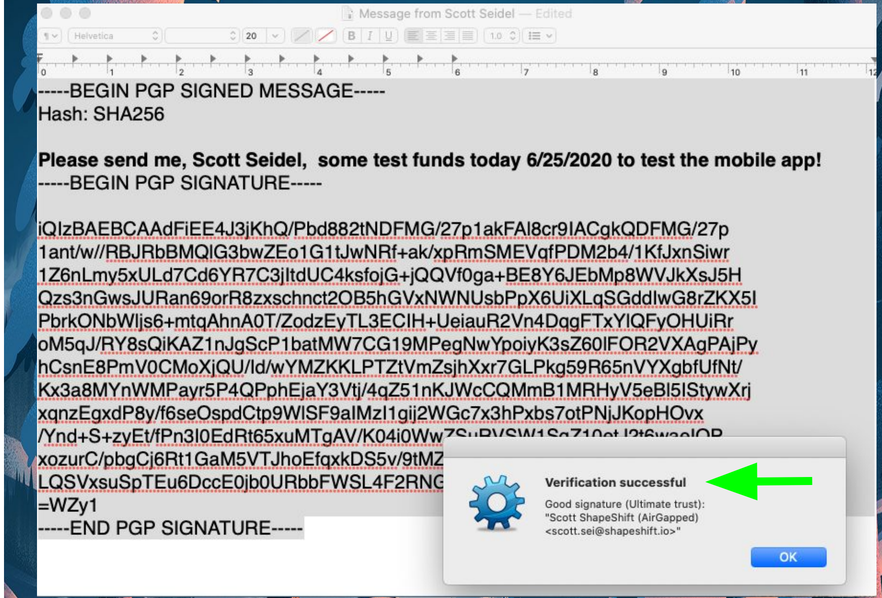

TextEdit
File
Edit
Format
View
Window
Help
Message from Scott Seidel
About TextEdit
Preferences... ⌘,
Services ▶
Hide TextEdit ⌘H
Hide Others ⌥⌘H
Show All
Quit TextEdit ⌘Q
Text
Add to Music as a Spoken Track
Convert Text to Simplified Chinese ^⌥⇧⌘C
Convert Text to Traditional Chinese ^⇧⌘C
Make New Sticky Note ⇧⌘Y
Open
Show in Finder
Show Info in Finder
OpenPGP: Decrypt Selection
OpenPGP: Decrypt Selection to New Window
OpenPGP: Encrypt Selection
OpenPGP: Encrypt Selection to New Window
OpenPGP: Import Key from Selection
OpenPGP: Insert My Fingerprint
OpenPGP: Insert My Key
OpenPGP: Sign Selection
OpenPGP: Sign Selection to New Window
OpenPGP: Verify Signature of Selection
Pictures
Import Image
Files and Folders
New Terminal at Folder
New Terminal Tab at Folder
OpenPGP: Decrypt File
OpenPGP: Encrypt File
OpenPGP: Import Key from File
OpenPGP: Sign File
OpenPGP: Verify Signature of File
Searching
Look Up in Dictionary
Search With Google ⇧⌘L
Services Preferences...

```
-----
Has
Plea                                 mobile app!
-----BEGIN PGP SIGN

iQIzBAEBCAAdFiEE4                    7p
1ant/w//RBJRbBMQIG                   iwr
1Z6nLmy5xULd7Cd6Y                    J5H
Qzs3nGwsJURan69or                    ZKX5I
PbrkONbWljs6+mtqAh                   iRr
oM5qJ/RY8sQiKAZ1n                    PAjPy
hCsnE8PmV0CMoXjQ
Kx3a8MYnWMPayr5P                     ywXrj
xqnzEgxdP8y/f6seOsp
Ynd+S+zyEt/fPn3l0Ec                  P
xozurC/pbgCj6Rt1GaM
LQSVxsuSpTEu6DccE
=WZy1
-----END PGP SIGNAT
```

GPG Practice Verification (continued)

Verify a message (Slack/TextEdit Example):

- Notice the Verification successful message that pops up from GPG



```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Please send me, Scott Seidel,  some test funds today 6/25/2020 to test the mobile app!
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEE4J3jKhQ/Pbd882tNDFMG/27p1akFAl8cr9IACgkQDFMG/27p
1ant/w//RBJRbBMQlG3bwZEo1G1tJwNRf+ak/xpRmSMEVqfPDM2b4/1KfJxnSiwr
1Z6nLmy5xULd7Cd6YR7C3jltdUC4ksfojG+jQQVf0ga+BE8Y6JEbMp8WVJkXsJ5H
Qzs3nGwsJURan69orR8zxschnct2OB5hGVxNWNUsbPpX6UiXLqSGddlwG8rZKX5l
PbrkONbWljs6+mtqAhnA0T/ZodzEyTL3ECIH+UeiauR2Vn4DqgFTxYlQFyOHUiRr
oM5qJ/RY8sQiKAZ1nJgScP1batMW7CG19MPegNwYpoiyK3sZ60lFOR2VXAgPAjPy
hCsnE8PmV0CMoXjQU/Id/wYMZKKLPTZtVmZsjhXxr7GLPkg59R65nVYXgbfUfNt/
Kx3a8MYnWMPayr5P4QPphEjaY3Vtj/4qZ51nKJWcCQMmB1MRHyV5eBl5lStywXrj
xqnzEgxdP8y/f6seOspdCtp9WlSF9alMzI1gij2WGc7x3hPxbs7otPNjJKopHOvx
/Ynd+S+zyEt/fPn3l0EdRt65xuMTgAV/K04i0Ww
xozurC/pbgCj6Rt1GaM5VTJhoEfqxkDS5v/9tMZ
LQSVxsuSpTEu6DccE0jb0URbbFWSL4F2RNG
=WZy1
-----END PGP SIGNATURE-----
```

Verification successful

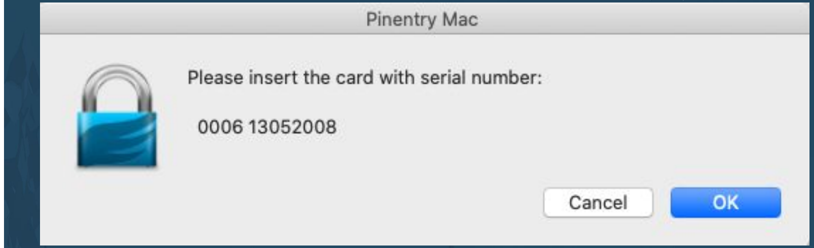
Good signature (Ultimate trust):
"Scott ShapeShift (AirGapped)
<scott.sei@shapeshift.io>"

GPG Practice Errors

Troubleshooting

- Is your Yubikey Present?
- Did you highlight the message?
- Do you know your 6 character Pin?
- Did you remember to “TAP” your yubikey?

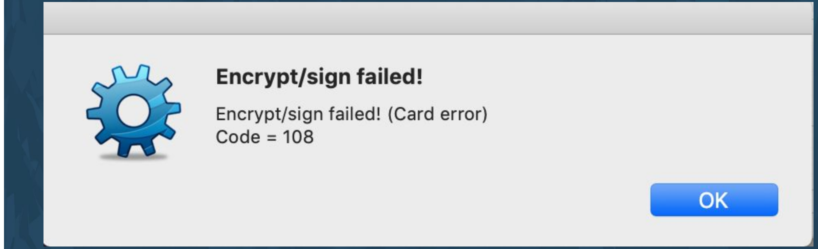
Yubikey is not found



Please insert the card with serial number:

0006 13052008

Forgot to TAP Yubikey



Encrypt/sign failed!

Encrypt/sign failed! (Card error)
Code = 108

Questions

Quiz

1. What are the Classes of Information at ShapeShift?
2. How do you treat Confidential information differently?
3. Why do we have alias emails?
4. When should you use your Alias email?
5. When should you use your Corporate email?
6. What is Strong Auth?
7. How do you perform Strong Auth?
8. When do you need to perform Strong Auth?
9. Why do we have a “Going Public” process?