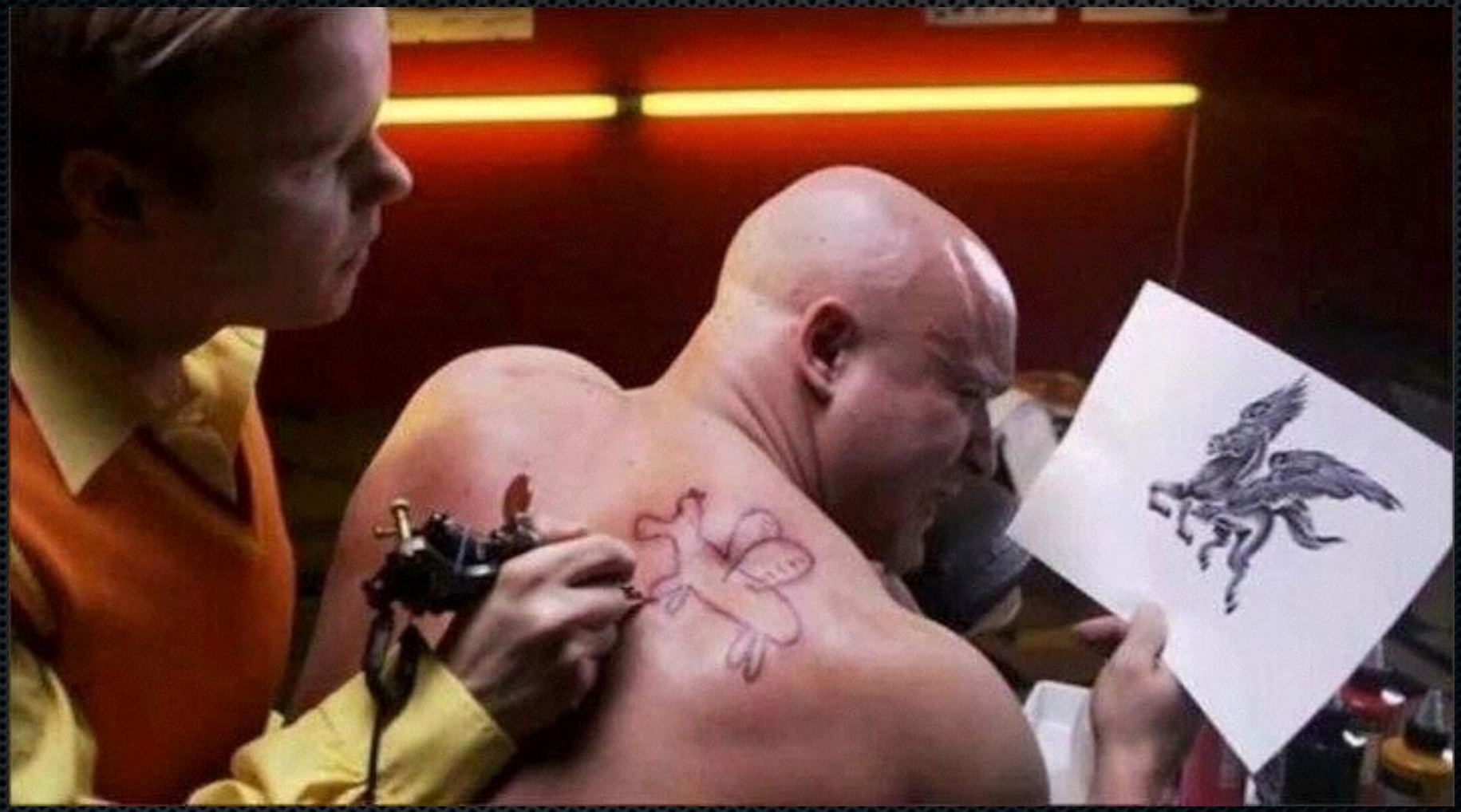
Security.
Keeping them out.

MACTECH

Why do we care?

How do we measure success?



Aren't Macs *inherently* secure?

MACTECH

- No

MACTECH

How do you get compromised?

- Phishing
- Weak passwords
- Missing patches
- Vulnerable runtimes
- Malware
- APT
- …

MACTECH

What can we do?

MACTECH

What can we do?

Security is trade-offs

- Understand the problems you want to solve
- Align interests and incentives
- Plan ahead
- Plan to fail

Depth and breadth

- Encryption – in transit, at rest
- System access
- Physical access
- Segmentation – networks, functions, people
- Policies, procedures, plans
- …

MACTECH

Weakest Link

MACTECH

25 most common passwords

Rank	Password	Change from
1	123456	Up 1
2	password	Down 1
3	12345678	Unchanged
4	qwerty	Up 1
5	abc123	Down 1
6	123456789	New
7	111111	Up 2
8	1234567	Up 5
9	iloveyou	Up 2
10	adobe123	New
11	123123	Up 5
12	admin	New
13	1234567890	New

Rank	Password	Change from
14	letmein	Down 7
15	photoshop	New
16	1234	New
17	monkey	Down 11
18	shadow	Unchanged
19	sunshine	Unchanged
20	12345	New
21	password1	Up 4
22	princess	New
23	azerty	New
24	trustno1	Down 12
25	0	New

MACTECH

Source: http://splashdata.com/press/worstpasswords2013.htm

UNCOMMON (NON-GIBBERISH) BASE WORD

ORDER UNKNOWN

Tr0ub4dor&3

CAPS?

COMMON SUBSTITUTIONS

NUMERAL

PUNCTUATION

(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)

~28 BITS OF ENTROPY

2^{28} = 3 DAYS AT 1000 GUESSES/SEC

(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS:

EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER:

HARD

correct horse battery staple

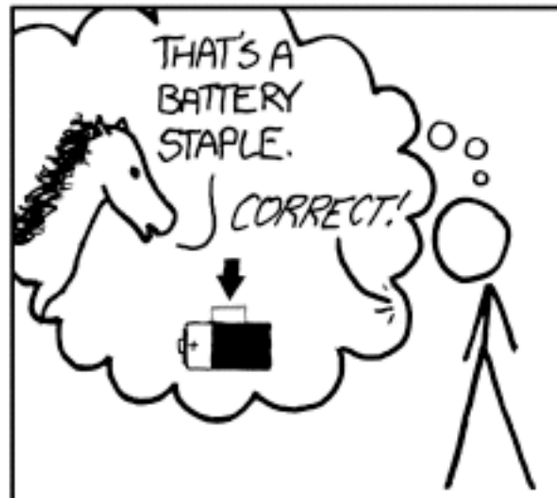
FOUR RANDOM COMMON WORDS

~44 BITS OF ENTROPY

2^{44} = 550 YEARS AT 1000 GUESSES/SEC

DIFFICULTY TO GUESS:

HARD



DIFFICULTY TO REMEMBER:

YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

UNCOMMON (NON-GIBBERISH) BASE WORD

ORDER UNKNOWN

Tr0ub4dor&3

CAPS?

COMMON SUBSTITUTIONS

NUMERAL

PUNCTUATION

(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)

~28 BITS OF ENTROPY

2^{28} = 3 DAYS AT 1000 GUESSES/SEC

(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS:

EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER:

HARD

correct horse battery staple

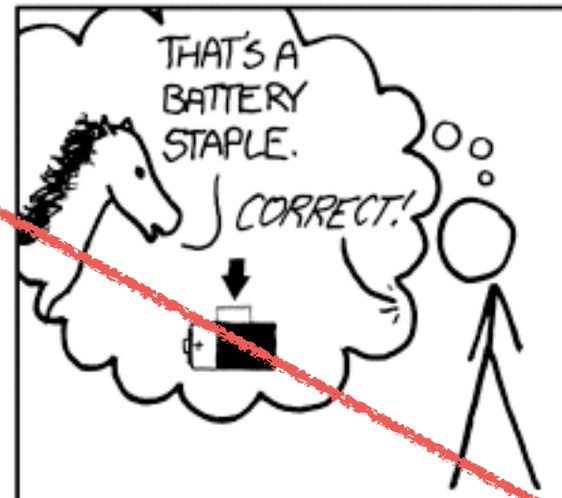
FOUR RANDOM COMMON WORDS

~44 BITS OF ENTROPY

2^{44} = 550 YEARS AT 1000 GUESSES/SEC

DIFFICULTY TO GUESS:

HARD



DIFFICULTY TO REMEMBER:

YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Passwords

- Consider the risks of compromise
- Don’t reuse passwords
  - Understand how passwords are compromised
- Password managers
  - Most people can’t remember enough strong passwords, but can remember one
- Password expiration can solve the wrong problem

Policies and Training

- Instill security mindset – "misuse cases"
- Social Engineering
- Incident Response

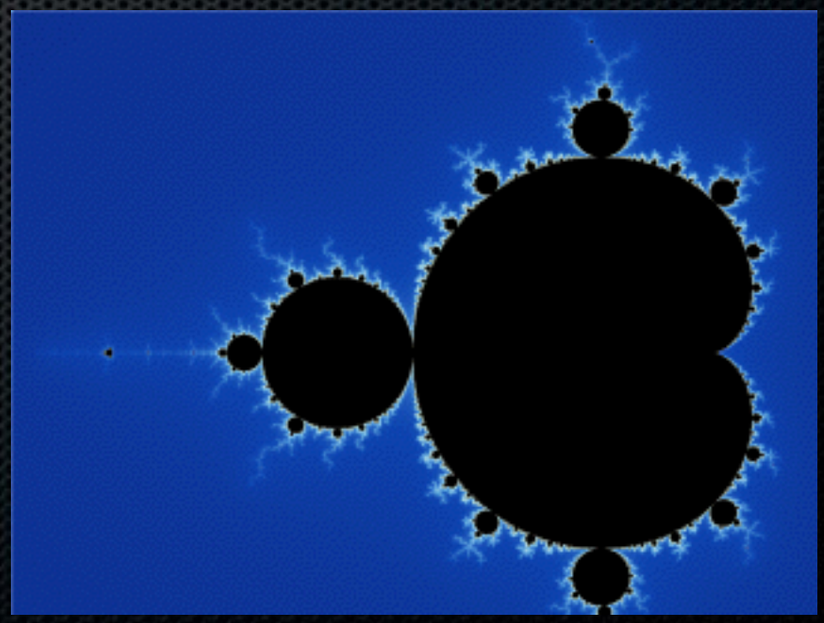
MACTECH

Encryption

- Full-disk encryption – FileVault, Data Protection
- Transport encryption – HTTPS, PGP, S/MIME
  - Key / Certificate management
- Authentication
- Ciphers, implementation, people
- Cross-platform access

Perimeter Security

1. Disable everything – in and out
2. Enable only necessary access
3. Repeat



MACTECH

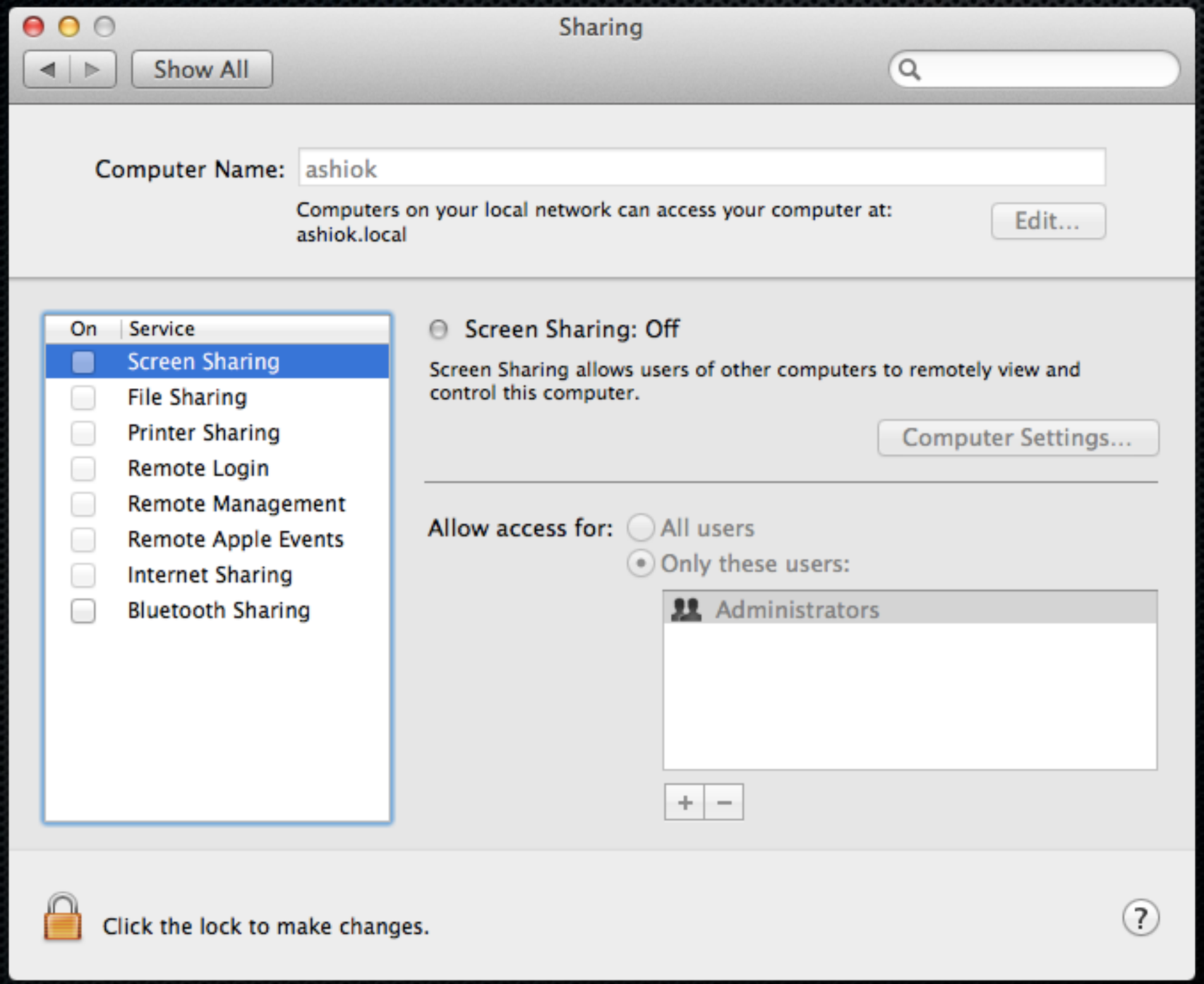
Network Security

- Disable everything – in and out
  - Network firewalls - deny by default
- Enable only necessary access
  - Track all changes to network access
- Repeat
  - The Internet-facing perimeter is not enough
- Trade-offs

Endpoint Security

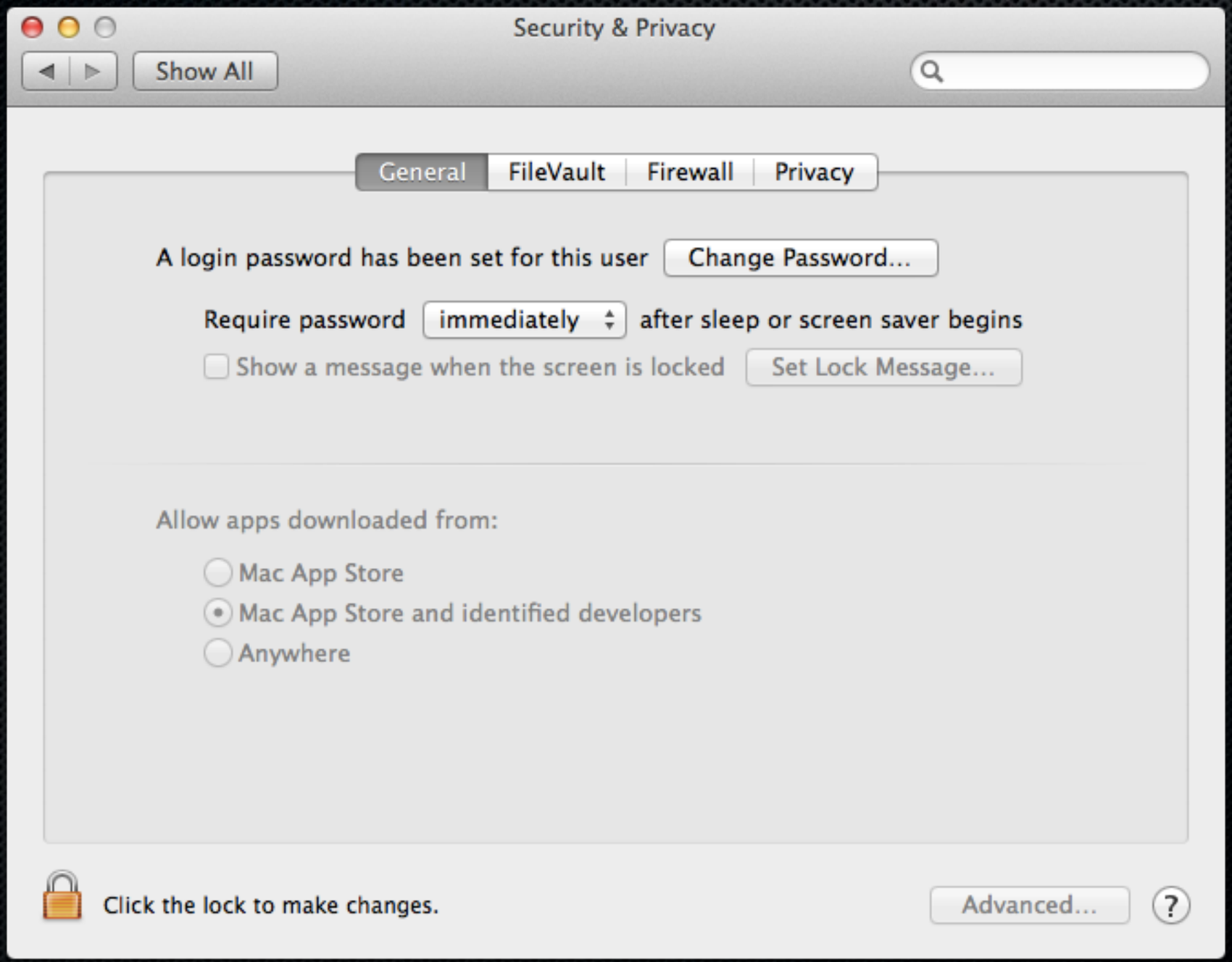
MACTECH

Endpoint Security



MACTECH

Endpoint Security

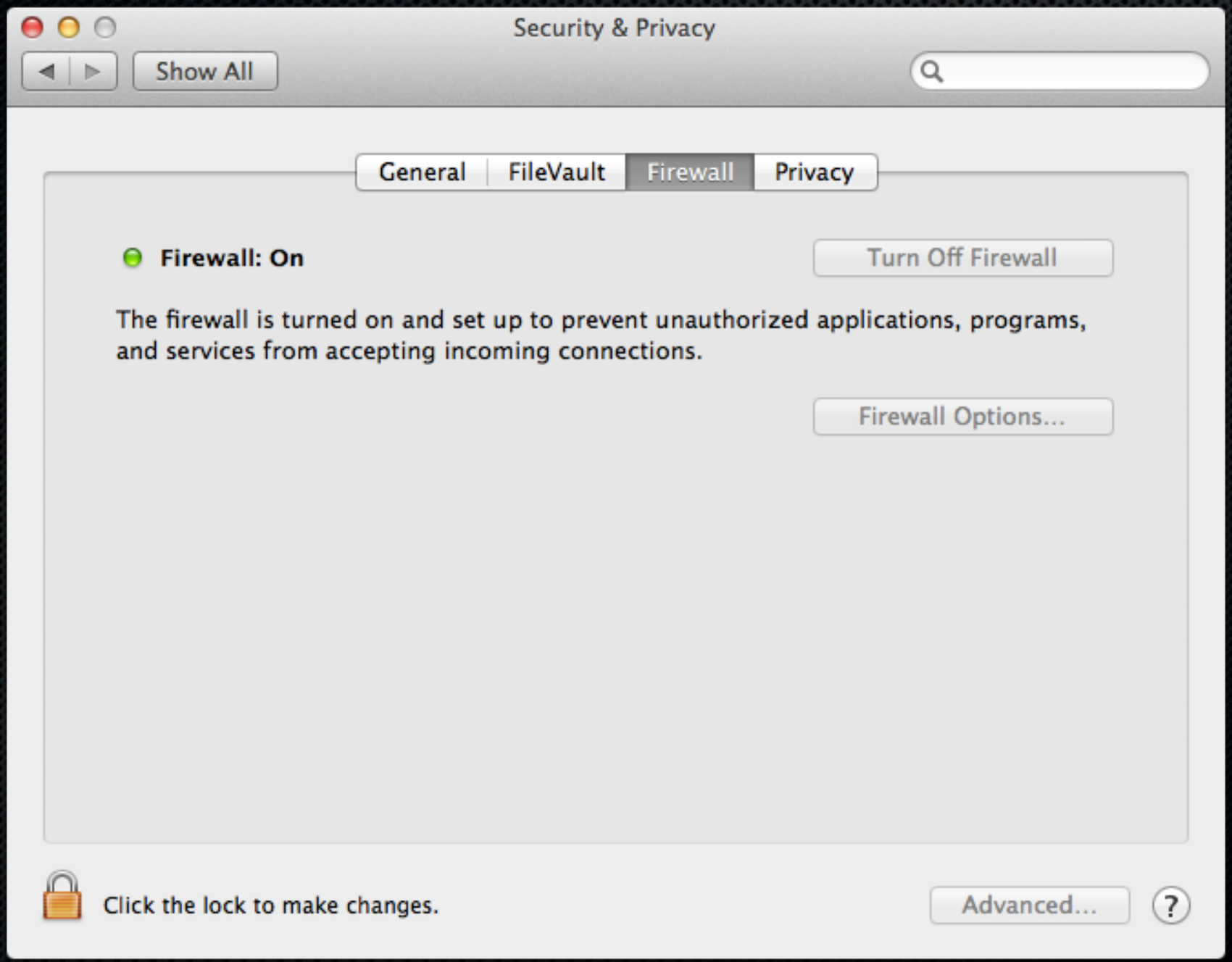


MACTECH

Endpoint Security

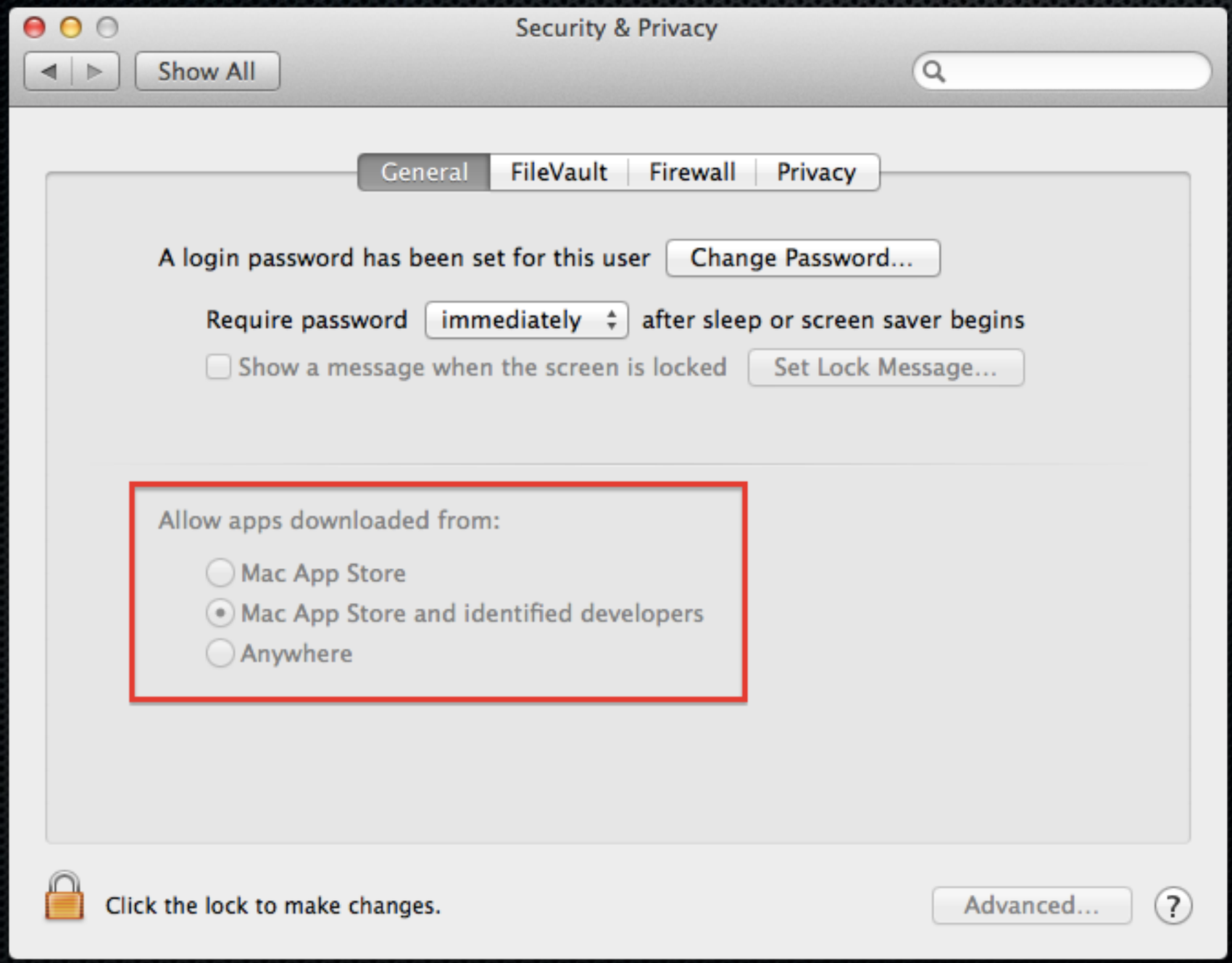
MACTECH

Endpoint Security



MACTECH

Endpoint Security

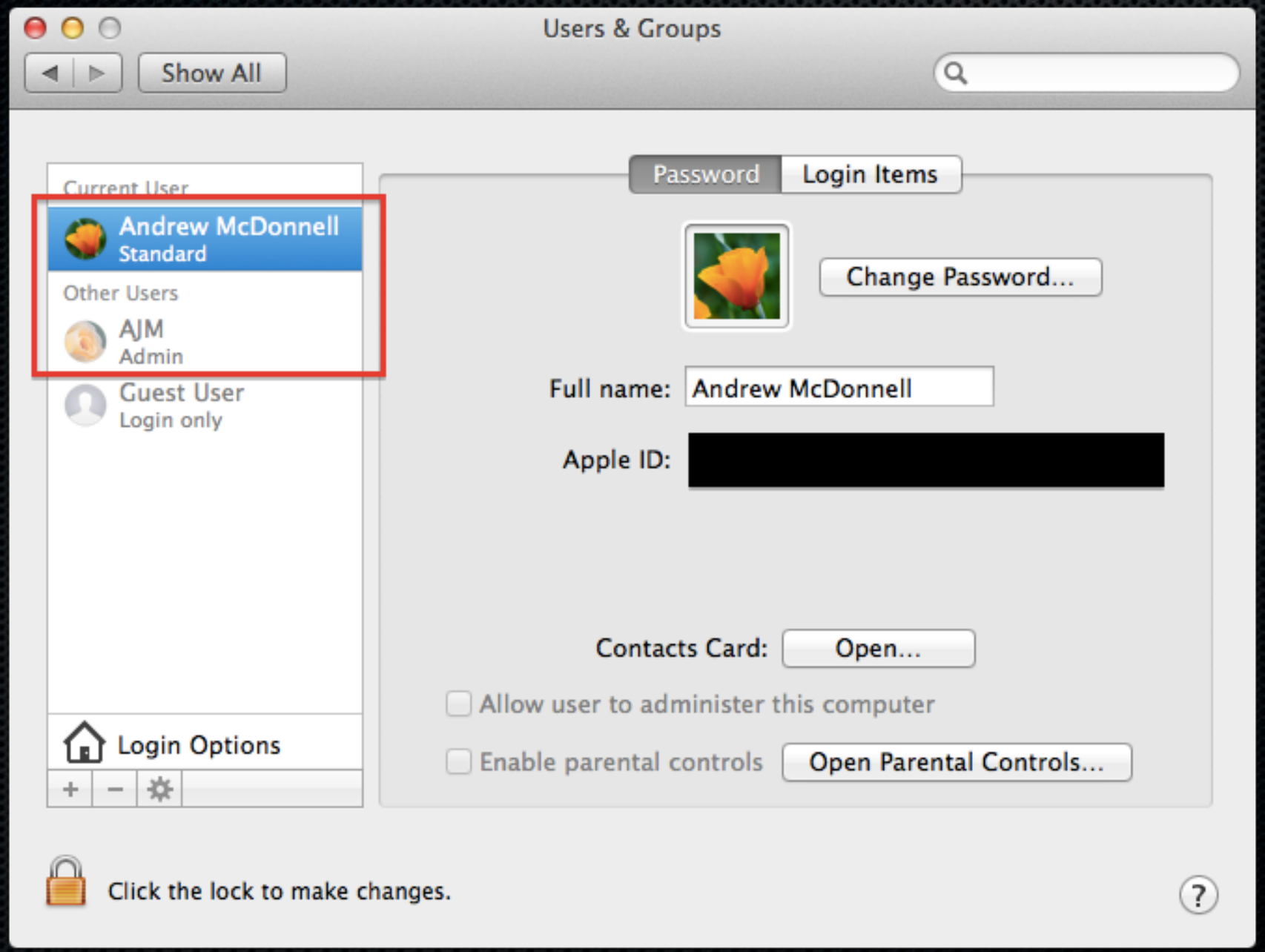


MACTECH

Endpoint Security

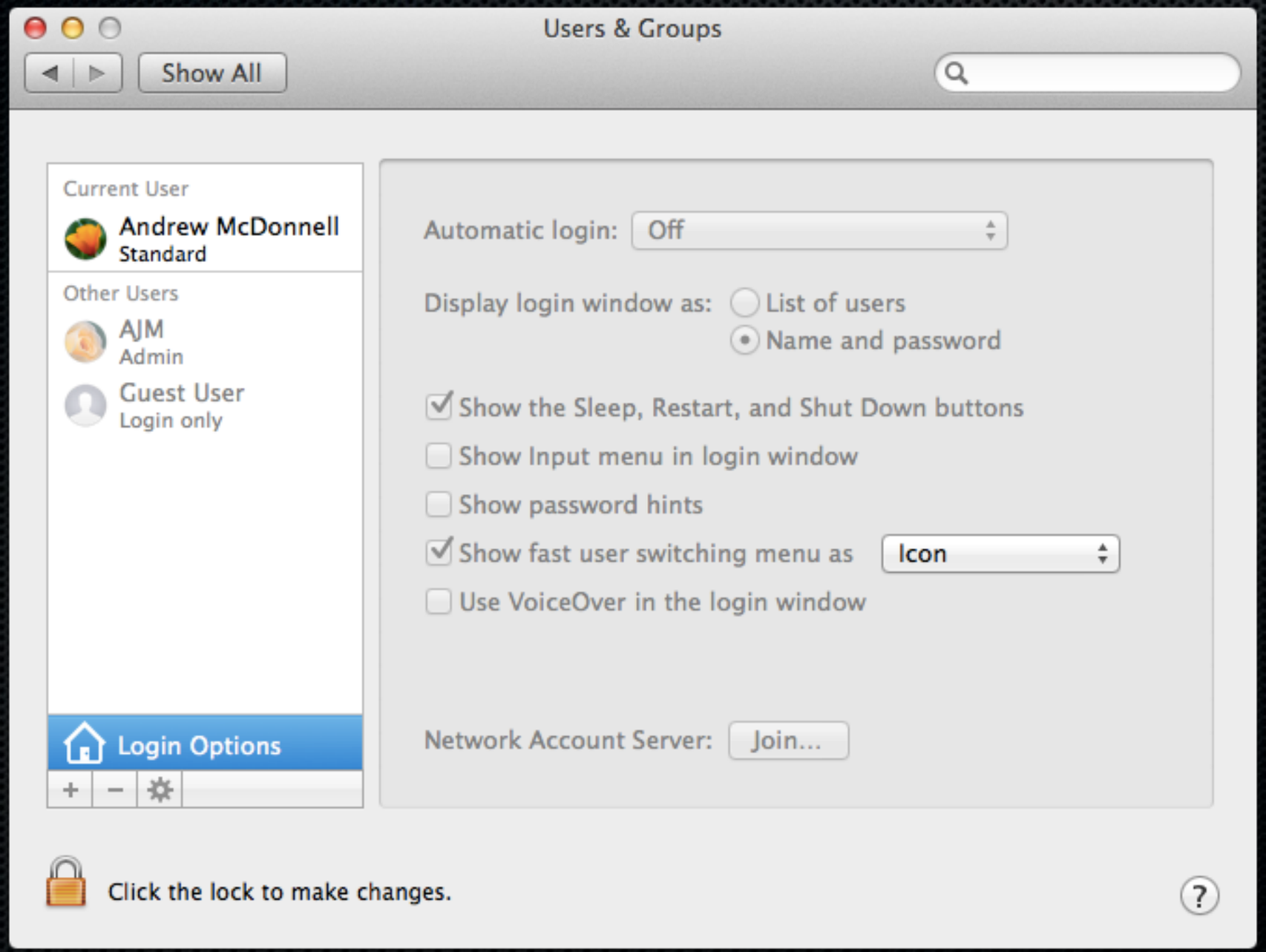
MACTECH

Endpoint Security



MACTECH

Endpoint Security



MACTECH

Endpoint Security

- Remove Java and Flash
  - Chrome includes Flash, Java only if essential
- Only join trusted, encrypted networks (WPA+)
- Think of hardware as your body

Security is hard

```
    if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;

    err = sslRawVerify(ctx,
                       ctx->peerPubKey,
                       dataToSign,                      /* plaintext */
                       dataToSignLen,                   /* plaintext length */
                       signature,
                       signatureLen);
        if(err) {
                sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify "
                    "returned %d\n", (int)err);
                goto fail;
        }

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
```

Questions?

Andrew McDonnell
andrew.mcdonnell@astechconsulting.com
510.270.5551

MACTECH