Mac Security in an Age of Cyberwar and Cyber Crime

Washington Apple Pi
June 25, 2011
Lawrence I. Charters

Mac Security: Physical, Mental, Spiritual

- Published in the Journal, 2005
- Linked from the opening page of the Pi site, http://www.wap.org/

ON HIRE FROM
CALEDONIAN SAFEMAKER
Tel 0800 001 007

Name your mac

- Mac's name should not be your name
  - Name it after a favorite goldfish or character in a novel
  - Name is entered in "Sharing" preference pane
- Hard drive name should not be Macintosh HD
  - Can be same or different from Mac name

Don't install unnecessary software

- For example, don't install X Window, even if it is included on the Mac OS X installation disk
- Be very wary of shareware or freeware that installs in menu bar, or installs Preference panes, or wants Internet access.
- If you don't use a piece of software, trash it.

Zur Beachtung!

Beachte die Gebrauchsanleitung für die Chiffriermaschine (H. Dv. g. 13).

1. Zur Sicherung der Walzenkontakte alle Walzen mehrmals gegeneinander vor- und rückwärts drehen.
2. Zur Sicherung der Tastenkontakte sämtliche Tasten vor Einschaltung des Stromes mehrmals kräftig hintereinander drücken und hierbei scharf lesen, sobald eine Taste dauernd gedrückt bleibt.
3. Bei Einstellung der in den Textsätzen vorkommenden Ziffern beachten, daß die Walzen richtig gerastet sind.
4. Die umzuwechselnden doppelpoligen Stecker sind bei zum Anschlag in den Buchsenspeere einzuführen. Der stärkere Hebelkipper ist deutlich zu schließen, da sonst 3 Lampen zugleich aufleuchten können.
5. Leuchtet bei Tastendruck keine Lampe auf, so sind die Batterien, der Kontaktfedern, der Ausschluß am Umkehrer und der Steckbuchse zu prüfen.
6. Leuchten bei Tastendruck zwei oder mehrere Lampen nicht auf, so sind die entsprechenden Lampen, die Kontakte unter diesen, die Kabel der doppelpoligen Stecker, die Steckerbuchsen einschließlich ihrer Kontaktfederchen, die Walzenkontakte, die Achsenkontakte unter den gerade gedrückten Tasten und die Rückkontakte unter den mit ihnen korrespondierenden Tasten zu prüfen und bei etwa notwendigen Verbindungen und Ersatzteilen zu ersetzen. (Siehe auch Ziffer 4.)

Von Maschine Nr. A 4388 ab dient zur Lampenprüfung die Öffnung mit der rechten Lampenfeldtaste.
Von Maschine Nr. A 4381 ab dienen zur Kabelprüfung die äußerste linke und rechte Buchse der mittleren 8er am Steckerbrett und die Kabelschlüsse auf den linken Lampenfeldtasten.

7. Walzenstellung und Walzenlagenfolge sind sorgfältig zu kontrollieren und die übrigen Impressionen hin und wieder auf ihren Sitz und einwandfreien Ob-Stände untersuchen. Die linken Kontakte der Walzen sind alle 6 - 8 Wochen mit Polierpapier oder in schärfen und mit einem wenig getränkten Öltupfer abzuwischen. Die Steckerbuchsen, die Lampenkontakte und die Kontaktfedern der sind wie Ob zu schützen.

8. Schäden hauptsächlich Schäden entstehen durch Fehlen oder Beschädigen.

Zum Umsetzen der Ziffern in Buchstaben oder umgekehrt dient nachstehende Tafel.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

DIRECTIONS FOR USING T

TO ENCRYPT:

1. Write down beginning rotor settings.
2. Type name or short message slowly (Plain Text).
3. Write down each letter as the light comes on (Cipher Text).

TO DECRYPT:

1. Return rotor settings to original settings.
2. Type in Cipher Text.
3. Write down Plain Text as light comes on.

NOTE:
Do not open the machine or move any of the dials.

Use unique account names

- If your name is Bob, the log-in name for your machine should not be "Bob."
- A first initial and full last name is more secure. Or a first name and last initial. Or something random, like "Berrybush"

Use unique passwords

- Forget nonsense about upper and lower case, numbers, special characters, etc.
- Passwords should be LONG (12 or more characters), and should not be associated with you personally.
- Passwords should be unique; **never use the same password for more than one service**.
- Use Password Assistance if necessary

Store passwords securely

- Use something like 1Password, or Keychain, or encrypted disk image
- Demo of encrypted disk image

Disable automatic log-in

- Absolutely vital for laptops, iPads, iPhones, iPod touch
- Should also do this for desktop machines at home. Keeps out children, relatives, visitors, maid service, plumber, painter, etc.

Every user should have an account

- Separate account for you
- Separate account for spouse
- Separate account for each child
- Separate account for visitor
- Delete unused accounts
- Disable "Allow guests to connect to shared folders"

For laptops, always set a master password

- Master password helps in recovery if laptop crashes.
- Not setting a master password can allow someone else to deny you access to your own computer by setting the master password and then encrypting your machine.

Disable Bluetooth

- Disable Bluetooth if you are not using it.
- If you are using it, turn off "Discovery" after you've synced your devices.

Disable AirPort

- If you aren't using wireless networking, disable it.
- Wireless is convenient. Wired networking is infinitely more secure - and faster.

Create an admin and a standard user account

- The admin account should only be used for things like system updates
- The standard user account should be used for day-to-day activities.
- The accounts should have different names and of course different passwords.

Careful about MobileMe

- Do not set up MobileMe for admin accounts
- Make sure your MobileMe password is strong; change it on your birthday.
- Make sure the MobileMe password is unique and not shared by any other service.

Make sure system time, date correct

- Vital for syncing between machines
- Vital for Time Machine backups
- Vital for system updates
- Vital for some kinds of security checks.

Install all system updates

- BEFORE installing updates, check system health, then
- Install ALL system updates
- "But I heard rumors that the new update melted pet kittens." Ignore the rumors; system updates are vital for security, whereas rumors are just rumors.

Set password for screen saver

- Set screen saver for a reasonable period (it should come on after 10-15 minutes of idleness)
- Require password to access after screen saver activated.
- Set Sleep corner for screen saver (recommend lower left corner)

Set security preferences

- Require password to wake from screen saver
- Disable automatic log-in
- Set master password on laptops
- Turn on firewall
- Optional: turn on stealth mode

Turn off everything in sharing

- Turn off file sharing, screen sharing, web sharing, etc.
- Turn on only when needed -- then turn them off again.

Enable check for updates

- Software Update "Check for updates - weekly" should be enabled.

Configure Time Machine

- Get an external drive.
- Turn on Time Machine
- Make sure it is backing up.
- Ignore it. Don't fiddle with it.
- If you have a laptop, a Time Capsule is even better: wireless networking and backup all in one box.

Safari

- Disable "Open safe files after downloading."
- Make sure downloads are always downloaded to "Downloads" folder.

Virus Checkers

- If you are required by work to have a virus checker, install whatever they recommend.
- For everyone else: try VirusBarrier Express, free from the Mac App Store. VirusBarrier Express can be set up so that it only runs manually, rather than all the time. If you have a concern, run it; otherwise, ignore it.