

Phamine – Opacity

- ❑ Secures web banking, web payments and cloud services
- ❑ Requires no website support (uses standard SSL/TLS)
- ❑ Prevents Phishing, website spoofing, key logging, etc.
- ❑ A true password safe - Protects your passwords even if your PC is hacked
- ❑ Only one simple PIN to remember yet each website gets its own very strong password

Phamine Opacity (patent pending) is a USB Internet security appliance that prevents ID theft through phishing, website spoofing, key logging etc. **without** requiring service provider support. Secure websites use the browser's encryption facility (SSL/TLS) to encrypt your login and other private information. This encryption is now performed in the Opacity device and your website login is submitted to the website by the device itself within the encrypted session.

Login protected from fingertips to web server

Even if the PC that you are browsing on has been hacked, the hacker will not be able to obtain your passwords. Your online passwords and other private information are submitted to the website directly through the Opacity device either by automatic submission (stored in secure memory) or by you entering the information directly on the device itself.

Only connects to legitimate web sites

Website certificates are verified by the Opacity device thus preventing website spoofing. The validity of the website is clearly displayed to the user on the device display.

Only one PIN to remember

If you choose the stored password option, you only have to remember the Opacity device PIN which enables you to use the device. Other models include fingerprint recognition and/or a smart card. This allows you to choose strong difficult-to-remember passwords for online usage or use the device to generate strong passwords for you.

A true password safe!

Software password safes are not secure from key loggers and other intelligent viruses and malware that may get onto your PC. Opacity provides a true off-PC password safe since the use of your passwords is only enabled by authenticating your identity directly on the Opacity device itself.

Trusted display for payment confirmations

Opacity can also be used to confirm beneficiary payments e.g. the LCD can be used to confirm beneficiary account creation in online banking. This prevents man-in-the-browser malware from manipulating the in-session transactions.

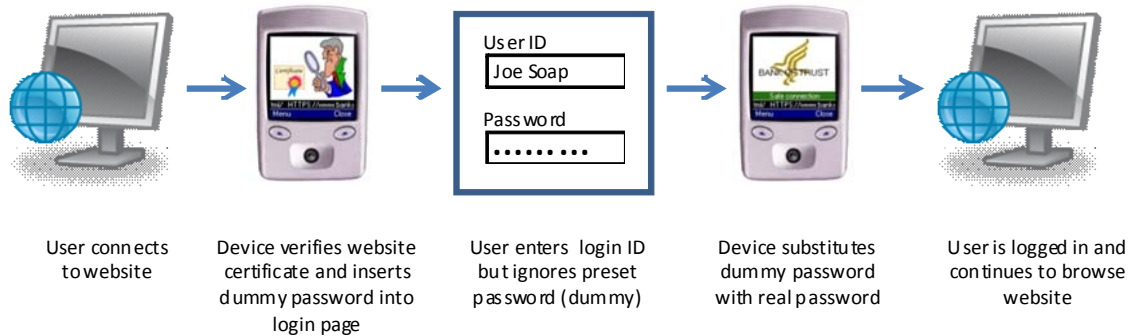
Secure backup of passwords

Depending on usage preferences, a number of simple secure password backup options are provided in case the device is stolen or lost.



Preliminary Phamine

Example login



User and service provider value

Users – are protected from modern Internet threats such as phishing, pharming, DNS re-direction, even a hacked PC i.e. password sniffing, man-in-the-browser, etc. Users are empowered with the control of their side of the security link in secure web sessions and don't have to depend on service providers for additional security. For instance banks make a business decision on how much to spend on customer Internet security, and while they may reimburse losses, they are not obliged to. Even if they do decide to reimburse, this would be preceded by (possibly highly protracted) investigations and the customer remains out of pocket in the interim. Phamine therefore works for users not service providers but benefits both.

Service providers – such as banks will benefit from the Phamine model as they are not pressured into additional security spending or taking on additional liability. They also don't have to become suppliers and supporters of IT equipment. Service providers and Insurance companies are therefore likely to encourage the use of Phamine devices.

Unfettered adoption

Only Phamine authentication devices provide strong hardware-based authentication from a user's fingertips to a web server without requiring additional back-end support. Phamine products are sold to users not service providers. Current hardware-based security solutions have to be sold to service providers ("service-centric"). These are generally all hard sales and this makes market penetration expensive and slow. Users are forced into service lock-in or having different devices per service. Phamine's "client-centric" model makes it immediately accessible to a market of almost 2 billion Internet users. Adoption is therefore unfettered by service provider control or apathy.

Use it anywhere

Internet banking fraud often begins in Internet cafes e.g. with PIN and password sniffing, however it is possible to safely use the Phamine method in this environment too. User's can launch a Phamine-aware browser from a write-protected USB disk (which may be built into the Phamine device). This requires no PC installation and allows users to safely use other PC's for secure logins.