LoginShield

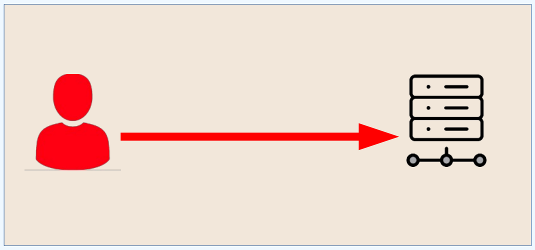
Our mission: empower organizations to eliminate the threat of password and phishing attacks on their users

OVERVIEW

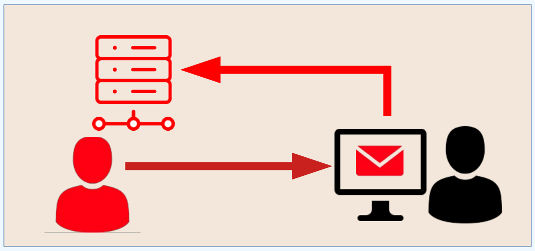
Two of the most common approaches involved in data breaches are attacking a user's password or tricking a user into disclosing the password to the attacker. Because these two approaches involve the user's actions, responsibility has generally been placed on users to actively protect their accounts.

An assortment of best practices related to password management and phishing attack detection, including the adoption of two-factor authentication and content scanning, have not solved the underlying problems. Passwords are useful in protecting a user's data and applications on a personal device, but they are not a secure mechanism for network authentication.

In this paper, we present LoginShield, a novel solution for authenticating users to network applications.



Weak passwords



Phishing

WHY CHANGE IS NEEDED

The number of people affected by data breaches each year is in the hundreds of millions. The average cost of a data breach varies widely, from under $10 million per incident for a typical small breach to over $100 million per incident. Many data breaches begin with password attacks and various forms of phishing, including business email compromise. The amount of knowledge and training required for users to be safe online has been increasing. Companies lack effective solutions to protect their assets and users from the most common attacks.

Passwords

Users are expected to choose and memorize strong passwords, rotate those strong passwords frequently, and avoid sharing the passwords with coworkers or other websites.

Phishing

Users must scrutinize every inbound communication to determine if the source is trusted and if the contact information presented is a legitimate website URL, telephone number, or email address.

At home

Websites may implement a two-factor authentication system to protect accounts with weak and stolen passwords, but users are still vulnerable to proxy phishing attacks. Websites increasingly implement password strength checks but still don't require users to rotate their passwords frequently. Websites face a dilemma because every additional security mitigation to protect customer accounts is also an increased risk of losing a sale or a customer due to inconvenience.

At work

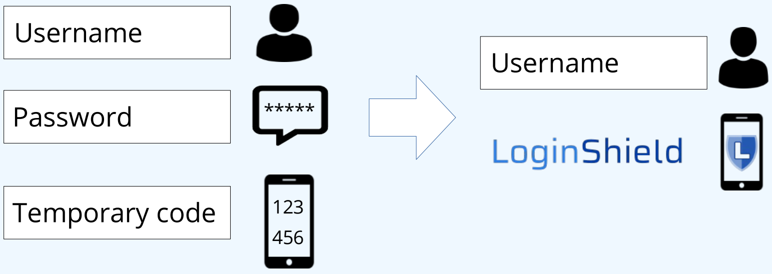
Companies may use email and website scanning solutions to warn or prevent users from following potentially malicious links. However, these techniques rely on heuristics and ever-growing lists of malicious domains, and as a consequence they cannot prevent all attacks. Furthermore, home users rarely install such tools themselves, leaving most Internet users vulnerable to password and phishing attacks.

LoginShield

LoginShield is Internet authentication 2.0

WHAT IS LOGINSHIELD?

LoginShield is a strong multi-factor authentication system with one-tap login and phishing protection. LoginShield is appropriate for authentication to network services such as web applications, email, and VPN.



Vulnerable to password
& phishing attacks

Secure one-tap login
with phishing protection

There are two significant problems underlying all password and phishing attacks. First, passwords are not a secure mechanism for network authentication. Second, a person can be tricked in a variety of ways to disclose their password or take some other action that would grant an attacker access to a protected resource. To protect users from password and phishing attacks, we need to solve these two problems.

DIGITAL SIGNATURES

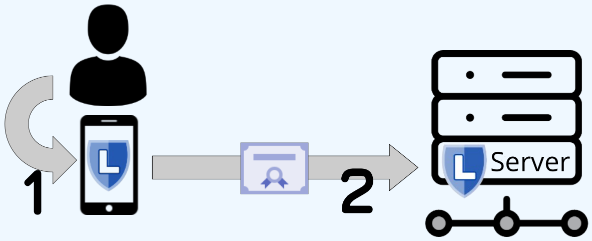
LoginShield uses digital signatures instead of passwords for network authentication. Digital signatures are a reliable and thoroughly tested technology that is already widely used for secure web browsing, email, and software distribution. LoginShield manages the credentials on behalf of the user, including creating new private keys and selecting which private key may be used for a particular authentication request.

SELF-SERVICE ENROLLMENT

LoginShield has a self-service user enrollment feature, making it easy to protect employee accounts on internal systems and customer accounts on a company's web, desktop, or mobile application. System administrators may configure LoginShield as an optional password replacement that each user can choose to enable, or as a mandatory authentication mechanism for all users.

MULTI-FACTOR AUTHENTICATION

LoginShield includes additional authentication factors, such as a local password and biometrics, to protect the use of the private keys used to generate the digital signatures.



1. Unlock app with passcode or fingerprint

2. Authenticate with digital signature

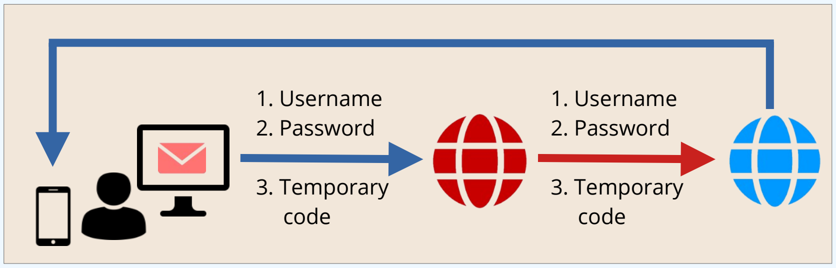
LoginShield

Secure and easy to use.
Eliminates credential-theft phishing attacks.

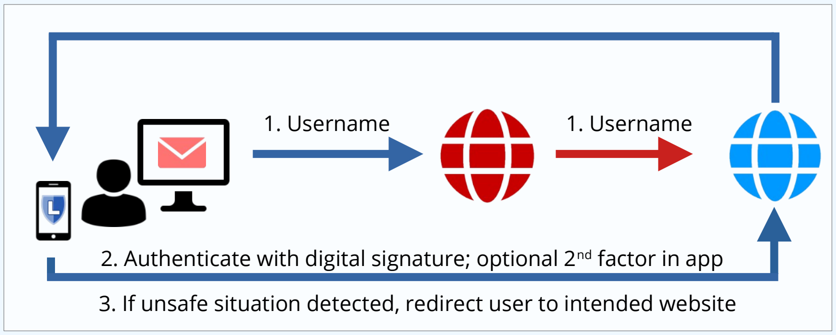
PHISHING PROTECTION

LoginShield integrates a phishing protection mechanism into the login process. This relieves the user from the burden of recognizing phishing attacks. In contrast to website and email scanning solutions that are always catching up to the latest attacks, LoginShield takes the opposite approach and checks each login request against a list of trusted sites that is automatically maintained by LoginShield for each user. Furthermore, when LoginShield detects a potentially unsafe situation, LoginShield redirects the user to the correct website. Instead of blocking the action, or merely warning the user that danger may be ahead, LoginShield circumvents the potentially unsafe situation.

Patent pending.



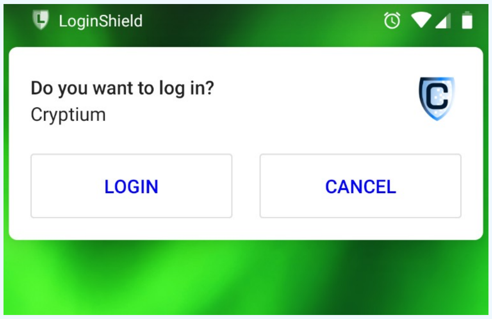
All 2FA using SMS, OTP, and push are vulnerable to proxy phishing


1. Username
1. Username
2. Authenticate with digital signature; optional 2nd factor in app
3. If unsafe situation detected, redirect user to intended website

Only LoginShield offers protection against proxy phishing attacks

ONE-TAP LOGIN

LoginShield has a one-tap login feature, making it convenient for every day use. One-tap login is available for routine authentication requests, and is not available during first time setup or when a safety redirect is needed to circumvent a potentially unsafe situation.


LoginShield

Do you want to log in?
Cryptium

ACCESS RECOVERY

LoginShield has an access recovery mechanism for situations where a user's authenticator has been lost, damaged, or stolen. Users must select at least one access recovery factor, and may select additional factors to increase the security of their account. Geolocation is available as an access recovery factor to permit access recovery only from specific places. Furthermore, when a user successfully recovers access to their account, LoginShield automatically blocks access from the lost, damaged, or stolen device. This prevents an attacker with a lost or stolen device from using any keys extracted from that device to access the user's accounts.