

PROSPER Login Enhancements

The PROSPER system is aligned with a number of security standards including Federal Information Security Act (FISMA) Moderate, HIPAA, and National Institute of Standards and Technology (NIST). As these standards evolve, security measures are updated accordingly. Two major enhancements are rolling out in the coming months:

1. Enhanced Password Complexity Requirements
2. Multi-Factor Authentication (MFA)

1. Enhanced Password Complexity Requirements

What's Changing

- Minimum length increases from **8 characters** to **15**, with a maximum of **64 characters** containing 3 out of 4 of the following: Lowercase characters, uppercase characters, digits (0-9), and one or more of the following symbols: @ # \$! % ^ & * - _ + = [] { } | \ : ' , ? / ` ~ " () ; .
- Password change frequency reduced from **every 3 months** to **once per year**
- **Bad-password database checks** will flag commonly used or compromised passwords and you will be prompted to select a different one if flagged

When users are next required to change their password, they will be prompted to meet the new 15-character minimum, while meeting the parameters spelled out above.

How to Create a Strong 15-Character Passphrase

Since passwords can now be kept for a year and possibly indefinitely in the future (unless a breach occurs), a passphrase is strongly recommended — easier to remember and significantly more secure than random strings.

Method	Example	Length
Three Random Words	BlueLawnChair7!	15 characters
Short Sentence	!!love!Braintree!	17 characters
Modified Quote	S@fetyFirst2026!	16 characters

Why a Passphrase?

- **Easier to type and recall** than random symbols
- **Mathematically harder to hack for a fraudster**, than a shorter complex password
- **Only needs to change** once a year or if your account is specifically at risk

2. Multi-Factor Authentication (MFA)

MFA adds a critical layer of protection beyond passwords alone and is required to maintain compliance. In the coming weeks, users will begin seeing prompts during login requesting a phone number for MFA enrollment.

Supported Authentication Methods

SMS text verification is the preferred MFA method when using a mobile phone — faster, more reliable, and better aligned with modern security standards than a phone call. Office/landline phones support phone calls only.

Method	SMS Text	Phone Call	Recommended	Notes
Mobile Phone	✓ Yes (preferred)	✓ Yes	✓ Strongly recommended	Preferred — supports SMS & calls
Office Phone/Landline	✗ Not supported	✓ Yes	⚠ Use if no mobile	Phone calls only — may not meet future requirements

MFA Frequency Policy

Scenario	MFA Prompt Frequency
Same device and browser	Once every 60 days
New device, new browser, or cleared cache	Immediately prompted

Rollout Timeline

1. Users will begin seeing phone number collection prompts at login in the coming weeks.
2. Users will identify the number as a mobile phone or office/landline phone.
3. After collection is complete, MFA will be rolled out board by board with direct communication to each group.

Phone Requirements & Limitations

- The Microsoft authentication service must be able to reach you directly.
- Mobile phones support both SMS text (preferred) and phone call verification.
- Office/Landline phones support phone calls only. Security standards in future will most likely not support office phones.
- The following are not supported:
 - Phone extensions
 - Shared reception numbers
 - Manual operators
 - Complex automated phone menus

Thank you for your patience and cooperation as we continue improving PROSPER system security.