

Quick Guide for Farmers



LONG & UNIQUE PASSWORDS

Username and passwords serve as the main way you can secure your different pieces of technology, and make sure the wrong person can't access your farm's accounts and systems. It's important to make sure that you take the proper steps to create a strong password, while also making sure you don't reuse this password in multiple places.

Username and Passwords

Your username tells the system who you are. Your password confirms it. Without the right combination, access is denied. Your password is often the primary barrier between your accounts and someone who shouldn't be in them.

An Easy Way to Manage Your Passwords

A Password manager can help you keep track of a strong, unique password for every account you have. It's an app that securely stores all of your login credentials in one place, so you only have to remember one password instead of dozens.

That single password — called your **master password** — is what unlocks access to everything stored inside. A **passphrase** works well here: a string of several unrelated words, like **HarvestMoonFencepost42**. Write it down and keep it somewhere physically secure, like a locked filing cabinet.

Installing a Mobile App/Using a Web App

Most password managers work on both computers and phones or tablets, and it's worth setting it up on whichever devices you use to log into accounts.

- **On a computer**, you'll typically install a browser extension that works alongside your internet browser like Chrome, Firefox, or Safari.
- **On a phone or tablet**, you'll usually download the app from the App Store (iPhone or iPad) or the Google Play Store (Android).

If you primarily manage accounts from your computer, start there. If your phone is where you do most of your logging in, start with that. The important thing is that you start small and continuously work towards migrating all your passwords into your password manager

FAQS

What does a strong password really mean?

Avoid anything personal, such as your name, your farm's name, a birthday, a favorite animal. Attackers can find or guess that kind of information more easily than you'd expect. Your password manager has a built-in generator that handles this for you, so you don't need to come up with anything yourself.

What's wrong with using the same password everywhere?

When one account gets compromised, attackers will take those credentials and try them on other sites automatically.

Why are default passwords dangerous?

Those defaults are publicly documented and widely known, so attackers can easily find this information to log into your devices if they know what they're doing.

How do I reset a password?

Most login pages have a "Forgot Password" option that will send a reset link to your email. Follow the link, set a new strong password, and save it in your password manager before you close the window.

UPDATE YOUR SOFTWARE

Companies will occasionally release patches and updates to fix security issues and make improvements in their products. Just like equipment needs to be maintained, so does your software.

Take Inventory of What You Have

Before you can keep your software up to date, you need a clear picture of what's running on your operation.

- Computers and laptops used for farm management or administrative work
- Routers and networking equipment
- Connected devices like smart irrigation controllers, GPS systems, environmental sensors, security cameras
- Farm management, accounting, or precision agriculture applications

Check the Current Status

- **What version is it running?** Knowing the current version is what lets you compare against available updates.
- **Is it still supported?** Running end-of-life software carries real risk, and if something on your list is no longer supported, it's worth planning a replacement rather than continuing to rely on it.

Turn On Automatic Updates

Most devices and operating systems can download and install updates automatically, and for everyday devices this is the most practical way to stay current without having to remember to check manually.

Searching something like *"how to turn on automatic updates on [your device or operating system]"* will typically surface official guidance from the manufacturer.

For specialized software or offline equipment where automatic updates aren't an option, the same approach applies; check the manufacturer's website or reach out to your vendor for guidance specific to that equipment.

What Are The Requirements

Some updates require a lot of storage space. Depending on the update or the device, your requirements could change. In general, check the following before running a major update:

- **Storage space.** Large updates need room to download and install.
- **A network connection.** Larger updates involve significant data downloads. If you're on a limited data plan or a slow rural connection, it may be worth scheduling updates when you have access to better connectivity or running them during off-peak hours.
- **Time.** Some updates install in minutes; others take considerably longer. Plan accordingly by including some time in your morning routine to check if your critical devices are up-to-date.

How Updating Works Differently Depending on the Device

Connected devices — computers, phones, tablets — can usually update automatically over the internet. For most of your day-to-day technology, turning on automatic updates largely handles this.

Equipment that operates offline or on isolated networks is a different situation. Precision ag tools, sensors, and embedded controllers may not connect to the internet at all, or may only connect periodically. Updates for these devices often need to be applied manually, either by you or by a technician, and through a physical method like a USB drive.

When an offline device reconnects to a network, it may attempt to download pending updates at that point.

Different Ways To Update

- **Over the internet** is the most common method.
- **From a website download.**
- **Via USB or physical media.**

Organizing and Scheduling Your Updates

A simple routine makes it easier to keep on top of updates. Once a month, spend a few minutes checking that your key devices are running current software. Add a check to your routine after any major equipment purchase or when you bring a new device online.

FAQS

What's a driver, and where do you find one?

A driver is a small piece of software that allows your computer to communicate with a specific piece of hardware — a printer, a GPS receiver, a camera.

Why does updating matter?

The most important reason is security. When a fix is released, the vulnerability it addresses often becomes more widely known at the same time.

A good example of this is ransomware, which is a type of attack where someone gains access to your systems and locks you out of your own files until you pay to get them back.

WATCH OUT FOR SCAMS & PHISHING

In today's digital world, bad actors are constantly trying to trick you into giving up your personal information. Knowing what these attempts look like is one of the more practical things you can do to protect your operation.

Think Before You Click

The most common way scams work is through a link or attachment in an unexpected message. It might be an email, a text, or a social media message that looks like it's coming from somewhere legitimate.

Before clicking anything unexpected, take a second to look closer.

Slow Down When Something Feels Urgent

Legitimate organizations like your bank, your lender, or a government agency generally give you reasonable time to respond and won't pressure you to act immediately.

If a message is pushing hard for a fast response, that's a good reason to slow down, not speed up.

When Something Feels Off, Ask Someone

If a message or request doesn't quite sit right but you're not sure why, ask someone else to take a look. A family member, an employee, or anyone else who's comfortable with technology can be helpful here.

Know What Legitimate Looks Like

The groups you work with regularly have standard ways of communicating with you.

When you know the normal routine, it's easier to spot when something is off. No legitimate company will ever ask you to share your password or read back a Multi-Factor Authentication (MFA) code over the phone or in a message.

Report It

If you receive something suspicious, report it.

Most email platforms have a built-in option to flag a message as phishing or spam. You can also report scam attempts to the Federal Trade Commission (FTC) at reportfraud.ftc.gov

ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

While strong passwords are crucial to protecting your assets, it's best to have another layer of protection in place. Enabling MFA on your accounts does this by requiring something more than just your password when you login.

The Different Types of MFA

When you log in with MFA enabled, you'll enter your password and then complete a second verification step. That step usually comes in one of three forms.

- **An authenticator app on your phone** generates a short numeric code that refreshes every 30 seconds.
- **A code sent by text message** is simpler to set up and widely supported.
- **A physical security key** is a small device, roughly the size of a USB drive, that you plug in or tap to your phone to verify your identity.

Technical Requirements

A cellphone or tablet is required for app-based or text-based MFA. For text message codes specifically, you'll need cell service at the time of login. Authenticator apps generate their codes locally on the device, so they don't require a connection at the moment you log in - which can be useful in areas with spotty coverage.

When to Use MFA

Turn it on wherever it's available. If you're deciding where to start, prioritize accounts where unauthorized access would cause the most damage, such as, your primary email account, online banking, farm management and precision ag platforms, and any accounts tied to operational data or business records. Your email is worth particular attention, since it's typically used to reset passwords, conduct business, and is tied to almost every other account you have.

FAQS

What happens when you can't access your MFA?

Most services provide backup codes when you first set up MFA. These are one-time codes meant exactly for situations where you can't access your usual second factor, like if you lose your phone or switch numbers.

How do you keep your MFA secure?

Keep your phone locked with a PIN, password, or biometric (face ID or fingerprint) lock. Beyond that, no legitimate company will ever ask you to read back your MFA code over the phone or in a message. If someone asks for it, that's a red flag worth taking seriously.

Why isn't a password enough?

Passwords can be exposed in ways that have nothing to do with anything you did wrong. Say you use the same email and password for your farm supply account and your online banking. Well, if that farm supply retailer gets hacked. Then the attacker now has your credentials!

With MFA enabled on your bank account, they hit a wall. They have your password but not your phone, so the login fails and you get an alert that someone just tried to access your account.

