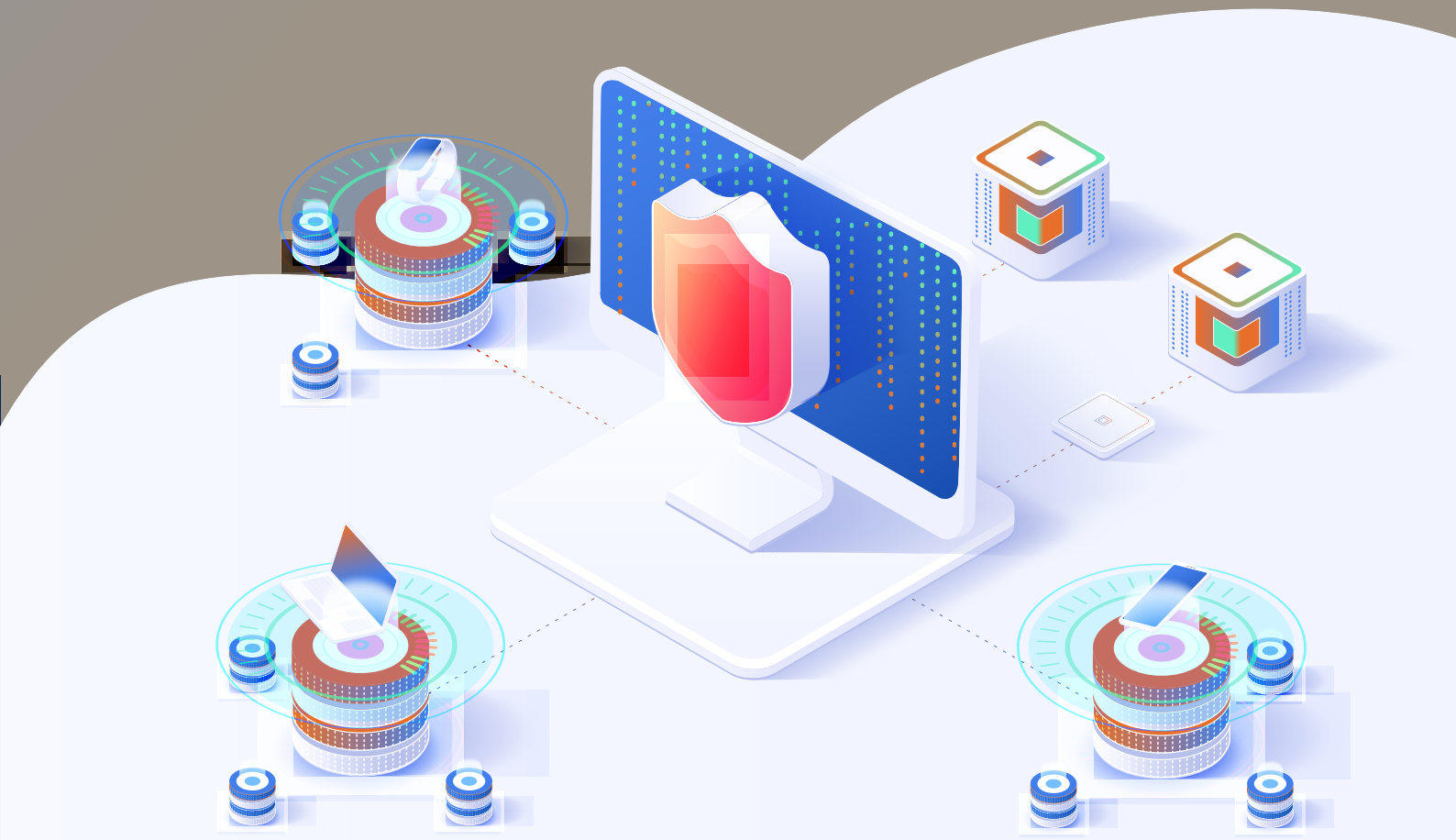
4 COMMON CYBERSECURITY MISTAKES

SMALL BUSINESSES STILL MAKE



GRIT TECHNOLOGIES

TABLE OF CONTENTS

Small businesses are not as safe as they think they are

Cybercriminals spare no one

There's a popular notion that only large businesses fall victim to cyberattacks. It's easy to see how this myth came about — the bigger the company, the more valuable data it holds.

However, the reality is that all businesses — even small ones — can suffer from cyberattacks.
Why? Because many small business owners believe they have nothing valuable for cybercriminals to steal, they hardly invest in cybersecurity. This makes them easier to infiltrate than large businesses that invest in robust technology.

And yet, many small-business owners feel confident in their cybersecurity efforts. In a 2021 survey by CNBC and Momentive, 56% of the respondents expressed no concern about suffering a data breach in the next 12 months. Almost 60% were certain that they could quickly resolve a cyber incident, but only 28% admitted to having a response plan in case of a cyberattack.

These are just some of the mistakes that increase small businesses' risk of suffering a cyberattack. In this eBook, we'll take a look at four other common cybersecurity mistakes and how you can resolve them.

Mistake #1: Failing to train staff in cybersecurity

One employee mistake can endanger your business

In the realm of cybersecurity, employees are typically considered the weakest link. Your business can implement multiple security solutions to prevent cyberattacks, but all it takes is one employee to make a mistake to compromise your IT systems. In fact, a recent study found that 88% of data breaches are caused by staff error.

Some say, however, that it's unfair to call employees the weakest link because it throws blame at them when managers also have a role to play in making everyone on the team more aware of cybersecurity.

Fix: Conduct an effective cybersecurity awareness training program

Cybersecurity awareness training aims to educate your staff about common cybersecurity problems and the roles they play in preventing and addressing these.

Training provides the following benefits:

- **Reduced risk of data breaches:** Various cyberthreats use social engineering techniques to trick people into clicking on harmful links and downloading malicious programs. Training your employees in cybersecurity best practices will make them less likely to fall for these tactics.

- **Increased client trust:** Cybersecurity awareness training improves your organization's ability to secure confidential customer information. Having the necessary cybersecurity certifications and credentials will make your clients more likely to trust and do business with you.
- **Time and money saved:** Cybersecurity training allows you and your IT staff to focus on more valuable things instead of spending time fixing the damages caused by a cyberattack.

Also, a recent IBM study has discovered that data breaches cost organizations an average of $4.24 million — enough to shut a business down. If your employees receive proper cybersecurity training, you can avoid paying such high costs.

Ensure the success of cybersecurity training by doing the following:

1. Assess your current cybersecurity landscape

Have your staff answer cybersecurity awareness surveys. Their answers will provide critical information on which areas of your company's cybersecurity initiatives are deficient and how you can fix them

2. Ensure everybody's participation

Everyone in your company — regardless of position or seniority — should participate in your cybersecurity awareness training program. By making cybersecurity everyone's responsibility, your staff will play a more active role in protecting your business from cyberattacks.

3. Be transparent

Before conducting cybersecurity training, call for a short meeting or send an email explaining its importance and goals, and how it will affect everyone's work.

During the training, always keep your employees in the loop by revealing future training plans and the progress the team has made since the training began.

4. Make the training relatable and fun

Don't just create slideshows for your cybersecurity awareness training and call it a day, as these may not resonate well with your employees. Instead, customize your cybersecurity training programs based on their roles, interests, and cybersecurity knowledge levels. Your training program will become more effective if your staff can relate with the training material.

Alternatively, you can gamify your training programs to make them more fun and to motivate your employees to do their part in your company's cybersecurity initiatives. Here are some ideas to try:

- **Cybersecurity Lab:** In this game, players need to strengthen the cyber defenses of a company experiencing sophisticated cyberattacks by cracking passwords and writing code.
- **Cyber-awareness challenge:** This game designed by the US Department of Defense requires players to promote awareness of cybersecurity issues and practice good cyber hygiene to prevent future events from happening.
- **Cyberattack simulations:** Stage a malware attack to see how quickly your employees can prevent their systems from getting infected. You can also send a fake phishing email to everyone and see who falls for it. Reward those who did well and provide a refresher course to those who failed.

5. Update and train frequently

Always review and revise your training materials and goals to keep them accurate and updated according to cybercriminals' latest techniques.

It's also ideal to conduct cybersecurity awareness training frequently. In a study by nonprofit organization USENIX, employees underwent phishing email identification training where they were tasked to spot such emails, at 4- to 12-month intervals. While the respondents easily spotted phishing emails four months after the training, they started forgetting what they learned after six months.

While cybersecurity awareness training frequency may vary among organizations, you can use the study's four- to six-month time frame as a starting point. At first, you might need to train your employees often so they can quickly retain vital information and develop good habits early. However, as your staff perform better in tests, you can conduct training sessions less frequently.

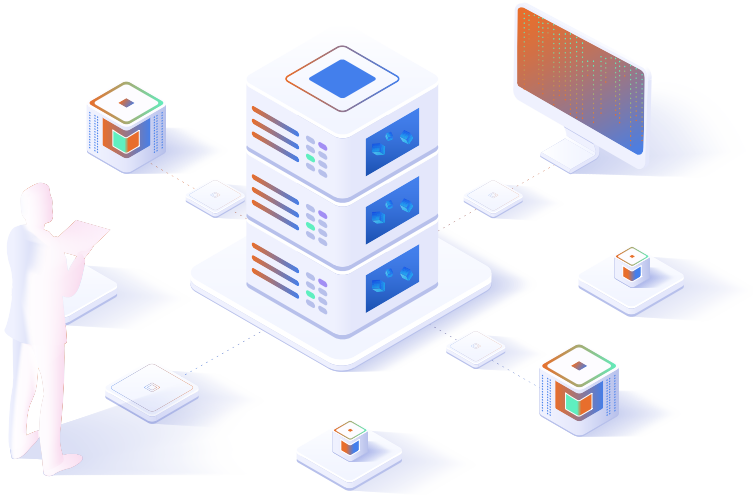
Mistake #2: Not having a disaster recovery plan

All businesses must have one

Disasters such as cyberattacks, natural calamities, and hardware and software failures are unpredictable. For instance, no one could have foreseen that the COVID-19 pandemic would take a toll on the operations of businesses worldwide.

And since many employees work from home today, they use their home internet connection to access corporate applications and data. This connection isn't as secure as corporate ones, however, putting organizations at risk of falling victim to cyberattacks.

It's therefore essential to have a proper disaster recovery plan (DRP). Unfortunately, only 54% of organizations have a company-wide DRP in place. If a business is unable to recover its data and systems after a major cyberattack, it runs the risk of paying hefty fines or closing its doors for good.



Fix: Make disaster recovery planning a priority

Take these steps to ensure that your business stays afloat when a disaster hits.

1. Identify your most crucial assets

Assess your processes and facilities to determine which data, programs, and hardware are needed to keep your business operational after a cyberattack.

You also need to establish a recovery point objective (RPO) and recovery time objective (RTO) for your crucial assets. RPO refers to the amount of data your company can afford to lose. So if you can only stand to lose two days' worth of data, your systems have to become functional within 48 hours of downtime.

RTO, on the other hand, is the maximum time it takes to restore your IT systems after a disaster. Your RTO can be as short as a few seconds for high-priority applications, as long as your IT department has a failover solution.

2. Create triplicate copies of your data

Your business needs to have at least three copies of your data. The first one is the original version that you currently use, while the second copy is an on-site backup saved on a disc, hard drive, or server. Finally, the third copy is an off-site backup typically hosted on the cloud.

With your on-site copy, you can quickly restore data since you have physical access to your files. Off-site backups come in handy when your on-site copy becomes unavailable because of data corruption or power outages.

Off-site backups should be stored in data centers that are at least 500 miles from where you keep your primary copy. This way, in the event of a disaster hitting your area, your off-site backups won't be affected. Having off-site backups also ensure you have clean copies of your data in case your systems are infected by ransomware.

3. Develop a disaster recovery communications plan

Having a communications plan will help you maintain your employees', customers', and stakeholders' trust in case disaster strikes. Here's how to create one:

- **Put people in charge of specific tasks.** Each department should have a point of contact who will communicate essential information to their teammates. Also, assign a team to oversee external communications.
- **Gather essential information.** Collect your employees' phone numbers, email addresses, and home addresses. Ask each of them to provide at least one emergency contact. Save the information you collected in the cloud so it's always accessible.
- **Prioritize.** Address first the concerns of employees and customers who were directly impacted by a disaster. You can tackle everyone else's issues after.
- **Create templates.** Communication templates make it easier to broadcast your message to different groups during a disaster. For instance, you can have a communication template that clarifies where employees should work during a disaster, who they're supposed to contact, and what information they're allowed to disclose to the public. Meanwhile, your customers have to know if they were affected by the disaster and need to take any actions.
- **Make sure everyone knows about your plan.** Call for a meeting regarding your disaster recovery plan so that everyone knows about it. Ensure that one or more copies of the plan are stored digitally or off site and inform the appropriate people where and how these can be accessed.

4. Train your employees and test your recovery procedures

Your workers are vulnerable to cyberattacks, so you need to regularly train them in disaster recovery best practices. For instance, teach them to avoid plugging in unvetted USB devices and other storage media into their business computers or mobile devices as these can contain malware.

You must also frequently hold dry runs of your disaster recovery plan and get your employees involved so they will know what to do during a disaster.

5. Conduct a postmortem

After recovering from a disaster, call for an incident postmortem with your team. Discuss how and why the incident happened, its effects and the measures taken to address the incident, and what should be done to prevent it from happening again.

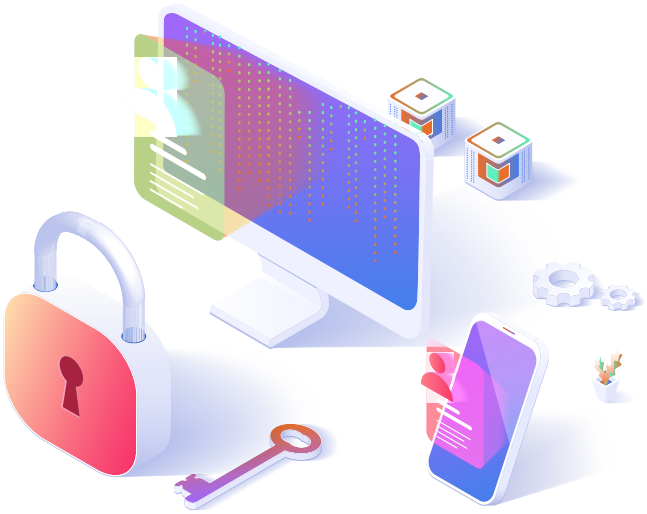
Mistake #3: Weak bring your own device (BYOD) policies

Allowing the use of personal devices for work can be dangerous

Today, employees use their personal laptops, smartphones, and tablets for work. Not only is this convenient, but it also allows them to work from any location with an internet connection. To regulate the use of personal devices, many companies implement a BYOD policy, a set of guidelines that define proper use of employee-owned devices.

A proper BYOD policy ensures the security of your company data even if your employees access it through their personal devices. A flawed one, however, potentially exposes your confidential information to cybercriminals.

For example, if your employees use a public Wi-Fi connection, attackers can exploit it to access your corporate network. Or if your staff's mobile devices are misplaced or lost, these may fall in the hands of criminals who can crack these devices' security to access critical data.



Fix: Develop a BYOD policy that works

Having a well-rounded policy can help your business overcome the security risks that come with allowing BYOD. To achieve this type of policy, you must do the following:

1. Make a list of approved devices

Identify the devices that will be permitted and supported by your company. Categorize approved devices by operating system, model, and age. At the very least, personal gadgets should be up to date and compatible with your organization's systems.

Restrict devices that are almost a decade old because they are more likely to have performance issues and break down. Do the same for gadgets running unsupported operating systems because their lack of security patches can expose your IT systems to cyberattacks.

2. Implement mobile device management (MDM) software

MDM solutions like Microsoft Endpoint Manager and BlackBerry UEM are designed to help IT departments monitor, manage, and secure company-registered mobile devices.

This solution has two key components: an MDM agent installed on a device and an MDM server. IT administrators manage cybersecurity measures through the server and transmit these to personal devices that have the agent installed on them. This gives IT admins the ability to separate corporate and personal apps on a user's device. It also enables them to wipe company data from a mobile device while keeping personal data intact if a user opts out of MDM or leaves the company.

Other MDM features include:

- **Application whitelisting/allowlisting and blacklisting/blocklisting:** Allows access to company-permitted applications while blocking applications deemed unsafe by security experts

- **Device inventory:** Displays a detailed list of each device's hardware specifications, operating systems, and patches so IT admins can easily provide support when issues arise
- **Remote troubleshooting:** Allows IT admins to remotely scan devices for issues and quickly resolve such issues
- **Over-the-air distribution:** Lets IT admins distribute updates and security patches to all company-registered devices
- **Password policies:** Encourages users to set strong and unique passwords to prevent account takeover
- **Location tracking:** Lets IT admins monitor a device's current location

3. Define acceptable use policies

Acceptable use policies refer to what employees are allowed to do with company data on company-regulated devices. These must cover the types of data employees are allowed to access and share outside the corporate network. Your policies should also define which websites and applications are forbidden during company time (e.g., social media websites, games).

Inform your employees that the company can and will monitor, access, and delete information from employee devices for the sake of the company's security and productivity, and what the consequences are for violating acceptable use policies.

4. Communicate your BYOD policy to all involved parties

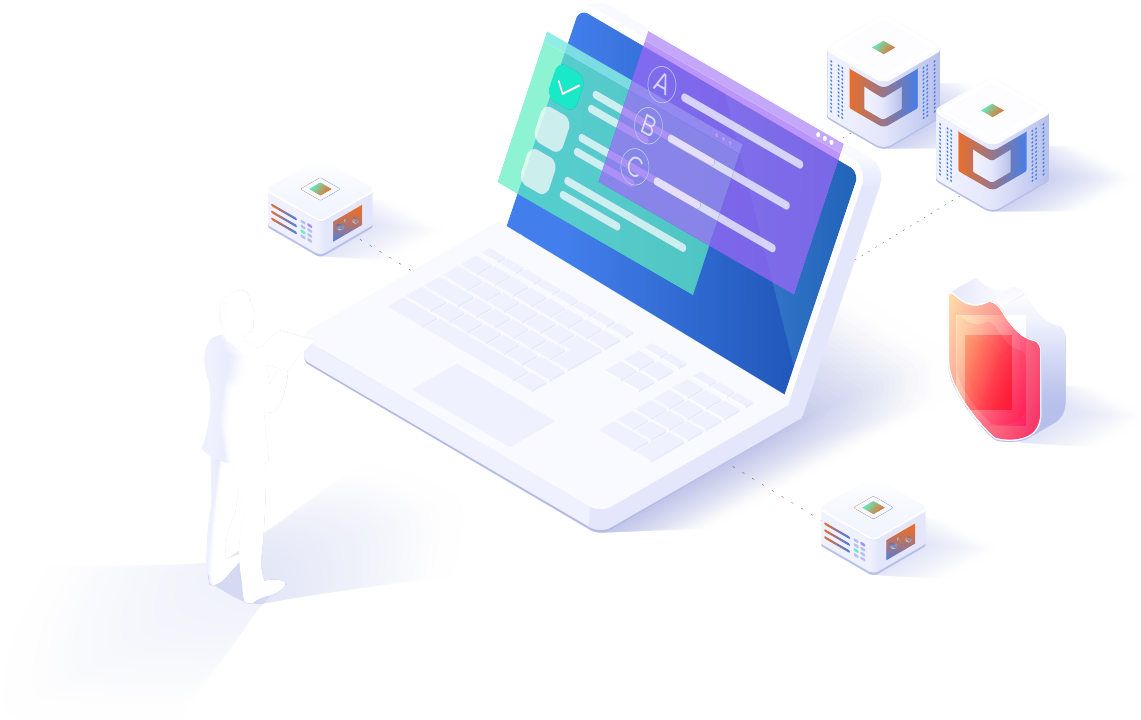
The success of your BYOD policy hinges on properly communicating it to all people involved. This way, participants are aware of their responsibilities and the consequences of their actions. Have all participants sign an agreement saying that they have read and understood your BYOD policy. Doing so protects your company from liabilities associated with employees who engage in inappropriate behavior using their company-regulated devices.

5. Train your employees

Provide comprehensive cybersecurity training to all participants of your BYOD program. Teach them good habits like securing their mobile devices with a PIN, fingerprint lock, or password, and refraining from connecting to unsecured networks.

6. Create an exit plan for your employees

Have a clear plan when employees leave the company or opt out of BYOD to mitigate the risk of data breaches. This typically involves uninstalling company applications, removing user accounts, and disabling access to cloud resources. If you need to delete company data, inform your employees first so they can back up their personal data to secure it from accidental deletion.



Mistake #4: Poor password habits

"passw0rd" is not a secure password

Passwords have long been used as a security measure to protect online accounts from unauthorized access. While they are effective in some ways, they are susceptible to hacking. In fact, Verizon's 2021 Data Breach Investigations Report found that passwords caused 89% of web application breaches, either through stolen credentials or brute force attacks.

To make things worse, many users have bad password habits, such as:

- **Using weak passwords:** Passwords such as "123456," "qwerty," and "iloveyou" can easily be cracked by cybercriminals in less than a second, but they are still widely used today.
- **Reusing passwords:** If a person uses the same password across multiple online accounts and that password gets exposed or stolen, then an attacker can use it to compromise all those accounts.
- **Writing down passwords:** It can be difficult to remember passwords, so some users write them down on sticky notes or their computer. Unfortunately, this method makes it easy for others to steal those passwords.
- **Using personal information as passwords:** Some people use personal data, such as names of family members, birth dates, street addresses, towns, and pets' names for their password. Doing so makes passwords easy to crack since hackers can easily acquire such personal information from social media sites and other online platforms.

Fix: Revamp your password policy

Fortifying your business's password policies mitigates the risks of cybercriminals infiltrating your employees' accounts using passwords. Here are some things you need to do:

1. Encourage the use of passphrases

Passphrases are a type of password that contain random dictionary words. These terms can be combined into one string (e.g., ducktaileducationsacredvelvet), separated by spaces (e.g., "follicle balcony cosmos unenvied," or mixed in with numbers (e.g., "bobsled23unnamed4jelly521 division").

Since passphrases typically contain unrelated words, they are harder for cybercriminals to guess but they're still simple enough for the account owner to remember. For instance, according to a passphrase generator website, it will take attackers 106,383,627,929 centuries to crack a password like "detonate pulsate avenge altitude" compared to 463 milliseconds for "qwertyuiop123."

2. Implement multifactor authentication (MFA)

MFA strengthens your organization's security by requiring users to enter two or more factors to verify their identity when logging into their corporate account. These factors are unique to a user and can be:

- Something they have, like a physical security key or a one-time passcode
- Something they know, such as a PIN or answer to a security question
- Something they are, like a retinal, facial, voice, or fingerprint scan

Even if a hacker gets a hold of an employee's login credentials, they won't be able to access the account without providing the subsequent authentication factor/s.

3. Discourage password reuse

Educate your employees about the dangers of reusing their passwords across their online accounts.

If they have trouble remembering their passwords, deploy a password manager, such as LastPass, 1Password, or Dashlane. Password managers log users into applications and websites automatically, eliminating the need to remember passwords. They also store passphrases in an encrypted vault that is only accessible with a secure master password.

Avoid these mistakes by partnering with GRIT

Let us help you make the right cybersecurity moves

Making even one of the mistakes mentioned in this eBook can compromise your organization's security. You may think that your in-house IT personnel can handle these issues, but their expertise may be limited. And while your data may be protected while they are in the office, what if a cyberattack happens while they're out? You will end up with no proper support, leaving your data vulnerable.

Fortunately, there's a solution: managed IT services providers like GRIT. We can function as your outsourced IT department through our professional team of experts who will maintain and monitor your IT infrastructure for cyberthreats 24/7/365. This way, you'll be protected even if you suffer from any cyberattack during off-hours. What's more, we can provide both on-site and remote IT support.

The best part? We will only charge you a flat monthly fee that's more cost-effective than paying a monthly salary to a full-time IT staff.

WE ASSURE YOU THAT PARTNERING WITH US WILL NOT BE A MISTAKE. CONTACT US TODAY!

Phone: **Detroit 586.286.8324/ Grand Rapids 616.251.1117** Email: **info@go.grittechs.com**

GRIT TECHNOLOGIES

www.grittechs.com