Staying **Safe** Online

A Practical Guide to Digital Security

Introduction

We are all connected. And whether you like it or not, a tremendous amount of your personal information is stored in systems around the world. No doubt you use at least a couple of devices that are connected. There is no escaping the rapid progression of technology.

As we have certainly benefited greatly from these significant advances, they have some down sides. While some of the smartest people living today are creating and leveraging technologies to improve our lives, there are many others that are exploiting these technologies, and wreaking havoc on our lives.

This booklet will help you identify steps you can take today that will reduce your risk. Staying safe online takes not one but many different strategic steps. And even with extraordinary efforts, there is no bulletproof solution. The ultimate goal is protecting your information, your privacy, and your money.

Cyber security is now a topic for every single individual, in and out of an organization. This is no longer something you can just count on your IT department or vendor to “handle”. This is your responsibility.

While this booklet is comprehensive, it is not exhaustive. Take the advice however you would like and know that there is always more that you can do to be safe. The intent of this booklet is not to supplant the need for professional cyber security resources, but rather to help you identify areas where you can improve your overall security posture.

Any mentions of products recommended are simply there for your benefit to help you find good solutions. You are encouraged to do your own research and find and partner with cyber security professionals that can help protect you and your organization.

People and Technology

People often think of computer security in terms of security products, and there are many hardware and software tools that help keep computers—and their data — safe. But the most important element of cyber-security – and the one hardest to control – is the human element. People are most vulnerable to one of the biggest threats to cyber security – social engineering.

Social engineering is persuading people to volunteer confidential information or assistance that will help the hacker's plan of attack.

The danger of social engineering is that it can quickly invalidate all the hardware and software protection provided by security products. This can make you, your family, and your organization vulnerable to attacks and serious losses.

Social engineering attacks can occur in many ways. They turn up electronically – for example via email or instant messaging – on the phone, or in person

COMMON SOCIAL ENGINEERING APPROACHES INCLUDE:

Phishing email. This is a scam where an email user is tricked into revealing personal or confidential information. The scammer then uses that information to gain access to the user's system.

The phishing email often looks like a communication from a legitimate business and may even include a company logo. It's common to see grammatical and spelling errors, and there may be style and formatting differences from a legitimate company email. These emails generally ask you for personal information or include a malicious attachment or link.

By hovering over a link in the email, you can reveal the actual URL, and often identify that the target is in fact something else. To validate it, make sure it matches the legitimate company's URL.The best practice, if possible, is to reach out to the company using a previously valid address. Don't open/click a link if you have any doubt about the email's authenticity.

Business Email Compromise (BEC). BEC is a type of scam that tries to deceive the recipient enough to convince them to send something of value. They target employees with access to company finances and trick them into making wire transfers or purchasing gift cards. Sometimes the emails contain malware.

Some BEC emails look and sound identical to a legitimate email from the spoofed sender. They can use similar diction and the same email signature. It's usually presented as an urgent request because they want to convince recipients to send money before they question the emails authenticity.

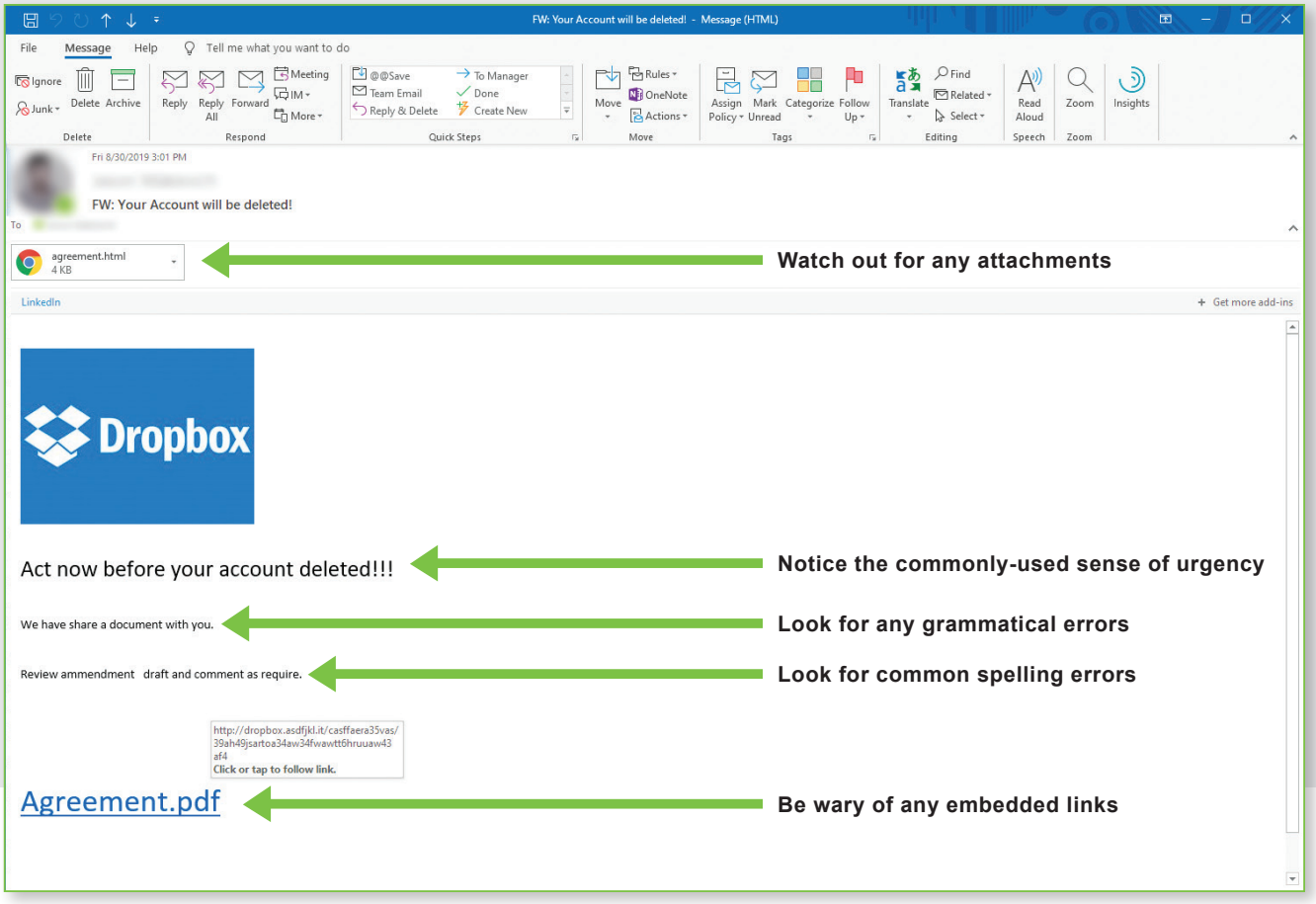
It is crucial for all organizations to enforce policies that require additional verbal or written authorization for any purchases or transfers of money.

USB Drop. Hackers have been known to drop infected USB thumb drives in parking lots of target companies, and various other locations. When an employee inserts it into their computer out of curiosity, it will execute its malicious program. Never insert an unknown USB into your computer.

Telephone scam. Someone calls from a seemingly legitimate area of your company or known vendor and asks for personal information like your password or credit card number. The outsider wants to hack into your system or use personal information for identity theft. Be sure to verify any requests like that by calling the individual back on a number you have independently authenticated.

Social engineering succeeds by finding the weakest link in the company. So, it's important to report any suspicious conversations or requests by outsiders.

Never give private information to someone you don't know. No legitimate person or organization will ever ask you for your password, PIN, or other similar piece of personal information.



This example of a phishing email points out some key elements that you can look for which may help you identify an email as fake. Remember, do not click on links or open attachments unless you are 100% sure they are safe.

Malware

The term "malware" is short for malicious software. Malware is software that is designed to damage devices, steal data, and cause problems. The creators of malware are looking to make money, either by spreading the malware themselves or selling it on the dark web.

Every individual and organization is unique, so it makes sense that different individuals and organizations will have different threats, different vulnerabilities, and different risk tolerances.

Risk boils down to how much you – or your online presence – are threatened.

Cyber risk can affect a company's – and an individual's – bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and retain customers. While malware runs silently, it can create symptoms that you may recognize. Keep in mind, none of these symptoms definitively mean you are infected. They just tend to make it more likely.

LOOK FOR ANY OF THE FOLLOWING SIGNS OF INFECTION:

- Changes to your browser homepage
- New toolbars on your browser
- Ending up on a strange site when searching for something online
- A change to your system settings (For example, your Windows Firewall is disabled)
- Pop-Ups appear
- New icons, programs, or website favorites that you didn't add or install
- Alerts about antivirus or firewall for products you aren't sure you have (many times these will be more generic alerts)
- Unexplained poor system performance

THERE ARE MANY THINGS THAT YOU CAN DO TO HELP PROTECT AGAINST MALWARE.

• Updates: Make sure all your devices, operating systems, and applications are up to date. Developers are constantly updating their products to patch vulnerabilities. Without these patches or updates, your system is vulnerable to infection or compromise. Attackers exploit these vulnerabilities quickly once they're discovered, so it is important to install updates quickly, very soon after release.

• Endpoint Protection: The devices that are most susceptible to malware are running Windows. While there are countless "antivirus" and "anti-malware" products on the market, it is important to look for products that employ several methods of mitigation, rather than simple, traditional signature-based antivirus. Look for an endpoint protection product labeled "next-gen" (next generation). They leverage a combination of techniques to help protect your system. None of the free security products on the market are adequate.

• User Policies: This especially applies to Windows systems. Make sure that you are not using your computer as a local administrator. If you can install a program without being prompted by Windows for alternate credentials, then your user privileges are too high. Create a separate user account with those permissions for occasions when you need them. But make sure that the account you use does not have those permissions.

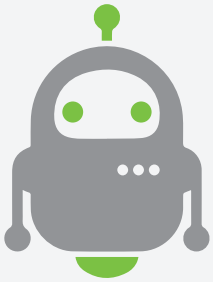
Types of Malware

BUGS

A flaw in the programming of a system or software. Oftentimes bugs present vulnerabilities to systems. A common threatening bug would be one on a website's source code that allows malicious action against the site.

VIRUS

A program that is designed to run undetected on a system which can then infect other systems and potentially cause damage or allow other malicious software to infect the system.



BOTS

Software that is preprogrammed to perform a specific function. Some bots are put on many systems (known as a botnet) and can be programmed to run a coordinated attack on a remote system.

WORMS

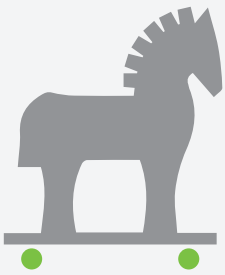
Malicious software that exploits hidden vulnerabilities, with the purpose of propagating to other systems and causing bandwidth and resource overflow.

RANSOMWARE

A program that when it is executed, will encrypt every file it can access with a key that only the hackers have. Then, the hackers leave text files in each folder with instructions (ransom note) on how to pay them (Bitcoin) so the user may recover their files.

ADWARE

Software that causes a system to popup advertisements. It is also possible that the advertisements could direct the user to a malicious site.



TROJAN HORSES

A normal-looking file that tricks the user into trusting it. Like the myth, this "horse" can contain malware.

SPYWARE

A program that can monitor and track a user's activity, including recording keystrokes so the remote hacker can capture usernames and passwords of many other systems.

The CIA *(no, not that one)* Confidentiality, Integrity, and Availability

Confidentiality. Integrity. Availability. These are the essential components of online security.

Confidentiality: Sensitive information is not disclosed to unauthorized individuals, entities, or processes. Your security measures need to make sure that not only your data is secure, but also your clients (or patients) data is secure.

One commonly-forgotten element of confidentiality is the "sanitation" of data. This means that when data is no longer needed, it should be completely removed from the system where it resides.

For example, the doctor's office you no longer go to does not need to have your medical information or your personally-identifiable information like your SSN or credit card number. They should have a process for sanitizing that information from their system.

Integrity: Important data must remain accurate. Malicious activity can change or corrupt critical data.

Availability: Your system must remain accessible and usable by authorized users.

A cyber security incident that attacks the availability of a system or data is called a "Denial Of Service" attack, or DoS. DoS attacks that impact many systems are called Distributed DoS, or DDoS attacks.

Today, the most common DoS attack to individuals and organizations is ransomware. This is a type of malicious software that encrypts data, in hopes that the data is important to the user or organization. If so, and the user or organization does not have a good backup, they may be forced to pay the attacker a ransom. This is typically transacted in Bitcoin, so they cannot be traced.

SOME COMMON ELEMENTS OF AVAILABILITY ARE:

Issues	Preventative Measures
• Hardware error	• Redundant systems
• Software bugs	• Redundant storage
• Environmental problems	• Redundant power
• A cyber security incident	• Redundant connectivity
	• Recovery solutions

Incidents

If you think your system has been compromised, seek the help of professionals.

TYPES OF INCIDENTS

A cyber security incident is an event that has an impact on the user or organization prompting the need for response and recovery. It usually impacts availability of your system, the confidentiality of your information, the security of your assets, and/or the reputation of you or your organization. Examples of incidents include:

• **Infection.** Your computer may be infected with malware.

• **Mass breach.** Corporations are constantly getting attacked, sometimes causing serious security breaches of their data If you have an account with any company that has been breached, you should take additional security steps immediately.

• Change your password. If you used the same password elsewhere, change those immediately as well.

• Monitor your bank account, credit card transactions, and credit history for any signs that your personal information was used improperly.

• Monitor the dark web through a reputable source for any compromised credentials. Consider using the free service haveibeenpwned.com

• **Company breach.** If you think your company's system may have been impacted by malware, a virus or anything that would affect your system's integrity, immediately contact your cybersecurity team or professional. You should have an Incident Response Plan already in place. A cyber security company can help you create that. Larger organizations should have a CISO, Chief Information Security Officer, who will take the lead on the response, with her or his team.
Many smaller organizations that don't have internal IT or cyber security resources often work with outside IT firms. It is imperative that you ensure these outside IT firms have an incident response plan for your organization and are trained and capable of handling any cyber security incidents.

Cyber insurance is another option to help mitigate the financial risks associated with cyber incidents.

Authentication

Just like physical assets like your home or car, your computing assets need a lock. With your computer or other electronic device, your password, passphrase, PIN, smart card, biometric fingerprint, or other mechanism is your lock.

It can be difficult to choose an effective password. It should be easy to remember but hard for anyone else to decipher. People have passwords for so many systems: corporate systems, online banking, voicemail systems, alarm codes, network password, system password, and many more.

Since it is can be tough to remember all these passwords, people sometimes use shortcuts like reusing the same password among multiple websites or writing the password on a piece of paper and putting it on their monitor or under the keyboard or mouse pad. This is extremely risky.

Commit your password to memory instead of writing it down. If you must write it down, keep it away from your computer and separate from the account name, preferably in a locked or secure location.

Don’t share your password with anyone. This includes your clients, vendors, partners, friends, coworkers, or even the system administrator. No one should ask you for your password.

Don’t use easy-to-guess passwords. Your maiden name, Social Security number or employee number, date of birth, your spouse’s, child’s or pet’s name–and of course, the word “password” are all easy to figure out. Always choose a password or combination of words to make the password easy to remember, but difficult for another person or computer to guess.

Password Tips

• Never use the same password in more than one system.

• Passwords should be complex.

• An 8-character alphanumeric password can be cracked in 3.4 minutes

• A 12-character alphanumeric can be cracked in96 years

• Use phrases. An example of a passphrase is Maythe4sBwithu! (but don't use that one now) :)

• Change passwords frequently.

• Don't save passwords in a spreadsheet on your computer!

• Post-it Notes are not considered secure.

• Consider a password manager/vault like LastPass, OneLogin, 1Password, or Dashlane. You will find that once you set one of these up, keeping very secure and unique passwords is easy.

To increase the difficulty of illegally accessing particularly sensitive resources—for example, your company payroll–you will need more than just a password. This is where you should consider using multiple-factor authentication or (MFA). Sometimes it's called dual-factor authentication, or 2FA. Of course, MFA can have more than two factors.
MFA typically combines something you:

KNOW You can know your password. If a hacker learns your password, then they "know" it just like you, and you have no other defenses without a second factor of authentication.

HAVE You can have a token (like a bank debit card, smart ID card or even your phone). Even if your password is compromised, the hacker doesn't have your token, and therefore can't access the system. Chances are, your phone is already often a token. Your bank may text you a six-digit code when logging in, and your phone becomes the token.

ARE This is a third factor which can be used in very serious systems. This would use something biometric, like your fingerprint or retina.

The more factors, the stronger the security. But more factors are also more costly, and time consuming. Consider apps and services like Duo, Authy, or YubiKey to make MFA easier and more secure.

Also, keep in mind what systems you have with access to others. If you want to reset a password on most systems, it will email you a reset link. So, if your email is compromised, then potentially so could your other accounts. Consider getting a security-minded email host, with MFA on your accounts.

Employee Behavior and Awareness

More than half of all cyber security incidents occur from within the organization. Employees, usually unintentionally, put their organizations at risk every day. This is often due to a lack of training and procedures.

Even with all the technologies organizations invest in, all it takes is the actions of one employee to put it at risk. One employee clicking on a link in an email. Or, connecting their personal device to the network or corporate VPN. Or, authorizing someone they think is “technical support” to access their computer. And the list goes on and on.

Some organizations invite cyber security experts to speak to employees about best practices. Unfortunately, most of that information gets lost in the day to day whirlwind of work.

Most organizations write and distribute policies that explain appropriate use and behavior with the organization’s systems. While it’s an absolutely critical component to any organization’s cyber security posture, on its own, it hardly mitigates the risks.
Fortunately, there are online learning platforms designed to continually train employees on good cyber hygiene. These platforms allow the organization to customize the content and delivery of training materials, which may be infographics, documents, and videos.

Most of these platforms also include testing components. They’re not limited to tests or quizzes that the employee takes after a lesson, although many of these platforms do include that feature. A more effective technique is a phishing test, where it will periodically send fake phishing emails to employees and will track any activity.

Cyber Security is Everyone's Job

YOU are responsible for cyber security. It doesn't matter if you are the boss, a manager, or an employee. Cyber security is everyone's job.

But, if you are the owner or manager, then you are the one accountable. Good cyber security requires buy-in from the very top. Without buy-in, your team will not consider this important, and your organization will be at much greater risk.

The NIST 800-171 is a widely-adopted framework within which all organizations should work. NIST, National Institute of Standards and Technology promotes innovation and industrial competitiveness by advancing measurement, science, standards, and technology. All US federal and most US state systems are required to follow the 800-171 framework, as are now most public and private enterprises in the US.

While this framework is complex, it is also comprehensive. If any organization intends to develop systems and/or processes based on this framework, it would be a tremendously difficult undertaking without outside professional assistance and guidance.

Go to nist.gov website for more information on the NIST 800-171 framework.

1 IDENTIFY

- Identify and control who has access to your business information
- Conduct background checks
- Require individual user accounts for each employee
- Create policies and procedures for cybersecurity

2 PROTECT

- Limit employee access to data and information
- Install Surge Protectors and Uninterruptible Power Supplies (UPS)
- Patch your operating systems and applications routinely
- Install and activate software and hardware firewalls on all your business networks
- Secure your wireless access point and networks
- Set up web and email filters
- Use encryption for sensitive business information
- Dispose of old computers and media safely
- Train your employees

3 DETECT

- Install and update anti-virus, anti-spyware, and other anti-malware programs
- Maintain and monitor logs

4 RESPOND

- Develop a plan for disasters and information security incidents

5 RECOVER

- Make full backups of important business data and information
- Continue to schedule incremental backups
- Consider cyber insurance
- Make improvements to processes/ procedures/ technologies

Business Security Checklist

Some recommended technologies and measures to help protect an organization:

- ☐ Firewalls (not the same as a router)
- ☐ Secure Remote Access
- ☐ Email Spam/Virus Filtering
- ☐ Encryption of all sensitive data
- ☐ SIEM or Syslog for Event Tracking
- ☐ Endpoint Protection (antivirus, firewall, etc.)
- ☐ Secure WiFi
- ☐ Internet Browsing Content Filtering
- ☐ Properly-segmented Networks
- ☐ Intrusion Prevention System

- ☐ We enforce strong password policies on every system, and ensure passwords are not stored insecurely.
- ☐ All of our devices, including mobile devices, laptops, and desktops are configured to prompt for a password or PIN after being idle for a few minutes.
- ☐ We use multi-factor authentication for all critical systems, including every email account.
- ☐ We have security policies that have been co-authored by our leadership team and a cyber security professional, are enforced throughout our organization, and reviewed at least annually.
- ☐ We have processes in place to ensure all our devices, operating systems, and applications are patched and updated shortly after these patches and updates become available.
- ☐ We limit access to every employee, including leaders and IT, so that no one can access anything they shouldn't, and cannot install any programs without being prompted for elevated credentials.
- ☐ We continuously educate our entire team, including every employee, on the latest cyber threats and best practices to promote proper cyber hygiene.
- ☐ We regularly test our entire staff by sending fake phishing emails through a phishing defense platform to monitor how each employee behaves when they receive one. This also includes following up with appropriate training for those that need additional help. This does not exclude anyone, including the business owner, from the testing.
- ☐ We have an incident response plan coauthored by our leaders, staff, and a cyber security professional, and have practiced it within the past year.
- ☐ We have a backup and disaster recovery plan co-authored by our leaders, staff, and an IT professional, and have practiced it within the past year.
- ☐ We have a mobile device management plan that requires any device with access to business systems to meet our strong security requirements and allows us to remotely wipe a device if it is lost or stolen.
- ☐ We have a cyber security firm review our security posture annually.
- ☐ We have cyber insurance.
- ☐ We monitor the dark web through a reputable service to alert us of any breached business accounts.
- ☐ We enforce procedures that require direct and personal interaction for any purchases, not allowing any purchases to solely be requested via email.

- **1 in 5 children** who access the internet have been sexually solicited.
- **1 in 4 children** who access the internet have seen unwanted pornography.
- Nearly **60% of teens** have received an email or instant message from a stranger -- **Half of them reply!**
- Nearly **62% of teens** report their **parents have no idea** at all what they do online.

Children and Cyberspace

The internet has become a vital part of learning for children in school. Much of their homework is online. Children now have better access to information than ever before.

But kids don't just use the internet for academics. They socialize online --sometimes even more than they do in person. As we all learn to embrace these changes -- some good, some bad, many we aren't sure of yet -- we need to be aware of the risks.

As with most parenting advice, good communication is key.

HERE ARE SOME THINGS THAT MAY HELP YOU IDENTIFY AREAS YOU CAN FOCUS ON:

• Discuss online behaviors and security risks. The more you communicate WITH (not to) your children, the less likely they will fall victim to the countless online threats.

• Talk frequently about practicing online safety. Offer guidance instead of trying to control children's online behavior.

• Discuss cyber bullying. Watch for changes in behavior. If your child suddenly avoids the computer or smartphone, it may be a sign he or she is the victim of cyber bullying

• Emphasize the concept of credibility and encourage children to proceed with caution. Teach them that not everything they see on the internet is true and people on the internet may not be who they appear to be.

• Talk with children and teens about the importance of creating and maintaining a positive online identity. What goes online today will be there forever. Think of everything you've ever posted online as your resume for life, that cannot be edited.

• Review security settings and privacy options for the websites your children use. Consider using content filtering services for every device your children use.

• Consider placing computers in a common area in the house.

• Spend time online with your kids.

• Set reasonable time and usage limits.

• Keep your children out of online chat rooms, and do your best to reinforce the rule, "don't talk to strangers".

• Teach them to never give out personal information online and to be careful what they post, including photos. Photos from a smartphone may contain GPS coordinates, which can inadvertently advertise where your children go to school, hang out, and live.

• Use a kid-friendly search engine instead of Google. Consider http://www.safesearchkids.com/ which is powered by Google,but safer for kids. This site also has a lot of useful information on this topic.

About Greenlight

Organizations large and small depend on technology more each day. The most successful organizations have learned to leverage technology to drive their business forward. Since 2010, Greenlight Information Services has been helping small businesses use technology to solve a wide array of issues and establish a competitive advantage in today's digital world.

Small businesses often think of their technology as a single component of their business. The small businesses that are growing faster than their competition are the ones that have treated their technology as a foundational layer of their entire organization. Greenlight challenges the status quo of their clients, enabling them to digitally transform every element of their business; their people, processes, and finances.

While so many IT organizations focus primarily on hardware, software, and uptime, Greenlight blends availability, strategy, and security in a way that spreads across the entire landscape of their clients' businesses. By learning where a business is now, and more importantly where the business wants to be, Greenlight strategically aligns technology and services to deliver proven results.

For More Information

If you would like to learn more about how to protect your organization, you may contact Greenlight by:

info@greenlight-is.com 949.359.0870 greenlight-is.com