Greengage

Cyber Security Essentials Guide

GREENGAGE GUIDE

Introduction

Why cyber security matters

While the internet offers numerous advantages, criminals are increasingly employing sophisticated methods to acquire individuals' credentials and data for financial gain.

Even if you diligently adhere to all recommended practices for safeguarding your passwords, there remains the risk of them falling into the wrong hands through targeted attacks or in the unfortunate event of a data breach at a company storing such information.

At Greengage, we prioritise the implementation of industry best practices to safeguard both your data and ours. We meticulously monitor and adhere to relevant security standards, including recommendations from the National Cyber Security Centre (NCSC). Additionally, we hold certifications for Cyber Essentials and Cyber Essentials Plus, meeting all the standards introduced in April 2023.

To enhance your personal data protection, we offer the recommended best practices throughout this guide, making it more challenging for unauthorised individuals to gain access to your sensitive information.

Greengage Passwords

How to create a strong password

Steer clear of using easily predictable passwords, such as key dates, family names, or pet names - while we take measures to block commonly used passwords, there are limitations to the number of passwords that can be restricted.

Refrain from using the same password across your significant accounts - this practice could potentially lead to unauthorised access if one password is compromised.

When creating a password, aim for a combination that is both memorable for you and not easily guessed by others. One effective method is to construct a password using three random words. For additional guidance, please refer to the National Cyber Security Centre (NCSC).

Protect your passwords

If you've documented your passwords, it's crucial to store them in a secure location—preferably out of sight and away from your computer.

Many contemporary web browsers include features for storing online passwords. These features are generally secure and often provide alerts when accessing a potentially "risky website" that might attempt to obtain your credentials. They may also warn you if the password has been exposed in a data breach, suggesting an alternative.

Consider utilising a specialised password manager from a reputable security provider. Additionally, make sure to back up recovery keys in case of a lost password for added security.

Greengage Passwords

2FA (Two Factor Authentication, also known as MFA – Multi Factor Authentication)

Many companies offer the option to set up Two-Factor Authentication (2FA). This ensures that accessing your account requires not only your login/password but also a 2FA code. We highly recommend implementing 2FA, especially on significant websites containing payment or confidential information. While most major vendors support this feature, only a few enforce it as a standard practice. Therefore, it's advisable to check within the site, typically in the account or profile section, to locate where to enable this security measure.

2FA codes can be delivered through various methods, including SMS text, Authenticator App, email, or phone call. Using an Authenticator App on a mobile phone is the recommended method. This adds an extra layer of security, requiring both something you "know" (e.g., login, password, pin) and something you "have" (e.g., 2FA/MFA).

Even if a potential criminal gains access to your login/password, without the MFA code, accessing your account becomes significantly more challenging for them.

What should you do if you believe you password has been stolen?

Promptly update passwords for any accounts where you've used the same password. You can utilise a website such as Have I been Pwned? by entering your email address.

This site compiles information on publicly known data breaches where your account details may have been compromised. Keep in mind that this resource only displays breaches that have been publicly disclosed, and there may be a delay before all breaches become widely known.

Greengage Pin Creation

Things you must not do

Avoid choosing easily guessable PINs or passwords, such as your date of birth. We proactively block commonly used and easily accessible PINs to mitigate the risk of fraudulent activities.

Exercise caution when sharing your device, particularly if banking apps are left open. Always ensure that any banking or payment apps are closed before handing over your device to others.

Before selling your mobile device or sending it for repair, make sure to delete any cards stored in e-wallets. For devices sent in for repair, it is highly recommended to back up the device, erase it, and then send it in. Providing a device for repair that still contains personal data poses a significant security risk.

If someone from Greengage calls you

In the event that Greengage needs to contact you, it is imperative to undergo a security verification process before discussing your account/s. This process may involve asking you specific information that only you would know, ensuring a secure identification.

It's crucial to note that no one from Greengage will ever call you to request your full PIN, password, passcode, or any other form of generated code. If you receive a call claiming to be from Greengage and asking for such information, it is advised to hang up and contact us directly using your registered number. Additionally, Greengage will never instruct you to transfer any amount of money, regardless of how small, to a new account as a means of verification.

General Best Practices

Public WiFi

While Public Wi-Fi offers convenience when away from home or the office, it comes with potential risks due to uncertainties about the security of the connected hotspot.

Some significant risks include:

- Malicious Hotspots
- DNS Hijacking: Genuine website queries may be manipulated to redirect users to malicious websites.
- Unencrypted Data Transmissions
- Malware and Spyware
- Man-in-the-Middle Attacks: Hackers can invisibly intercept all internet traffic.

We strongly advise against connecting to banking apps/websites when on public Wi-Fi, given the often-limited security. If urgent access is necessary on public Wi-Fi, consider the following precautions:

- Use a VPN: This establishes a secure connection between your device and the VPN provider, encrypting traffic independently of the network. Various types of VPNs are available, including full VPN clients and browser-based VPNs (though the latter may have limitations, leaving certain apps unprotected).

Computer updates

Operating system/application:

Maintaining up-to-date computers, phones, and tablets with the latest updates, particularly security updates, is of utmost importance. While some may find the process of updating their devices cumbersome, it is crucial for self-protection. Vendors routinely release updates to address security vulnerabilities promptly, and keeping your devices updated is a proactive measure against potential security attacks. Failing to update promptly may expose you to exploitation by malicious actors.

Endpoint protection (formerly known as anti-virus):

Running a computer connected to the internet, whether it's Windows, Mac, or Linux, without any protection is highly risky. Most Windows 10/11 devices come with robust built-in protection. For those without, or using Mac/Linux systems, it's essential to invest in security software from reputable vendors. While free editions are available, they may lack the more advanced protection features. Don't compromise on endpoint protection, as it serves as a critical defense against various online threats.

Mobile devices

We strongly recommend configuring iPhones/Androids with the following settings:

- Set a minimum 6-character PIN, avoiding simple combinations like 123456 or 000000.
- Register your device for Find My iPhone/Android Device Manager. This allows you to trace your device and, crucially, remotely erase it in case of loss, preventing unauthorised access to personal data.
- Avoid Jailbreaking or rooting your mobile device.
- Install only legitimate applications from the Apple/Google Play stores to ensure the security and integrity of your device.

Backups

We recommend backups of crucial data in alternative locations to guard against potential threats. A common cyber-attack involves malicious links or attachments that encrypt all your data, demanding payment - usually in cryptocurrency - in exchange for a decryption key. Even if the payment is made, there is no guarantee that the decryption key will be provided. The likelihood of receiving the key after payment is generally low, but individuals may still take the risk, especially if the content is exceptionally important.

This method is favoured by hackers due to its potential for high rewards with a relatively low risk of being caught. The primary defence is to have a backup of your data in a separate location, ensuring the ability to recover data without the need for payment.

Beware of Phishing Scams

The most prevalent phishing attacks occur through email, where attackers use deceptive information such as fake sender emails, web links, and cloned branding to create an appearance of legitimacy. To identify such phishing emails, watch out for indicators like poor spelling and grammar, suspicious URLs (hovering over the URL may reveal a legitimate display, but the link leads to a fraudulent address), and scrutiny of spelling, as attackers often acquire domain names with subtle misspellings of the original.

Phishing emails often create a sense of urgency, using terms like "urgent," "your account will be disabled," or setting a deadline to pressure recipients into swift action, aiming to prevent thorough inspection of the email. Remaining vigilant to these signs can help users identify and avoid falling victim to phishing attacks. The most common types of phishing scams include:

Baiting

This is a deceptive technique employed by scammers, involving the use of false promises or enticing offers to lure victims into a trap. The goal is to manipulate individuals into divulging personal and financial information or to infect their systems with malware e.g., a seemingly appealing attachment which conceals malicious intent.

Spear phishing

When your card is stolen, not only can your card be used by the thief to make unauthorised payments, your details are also at high risk of being sold onwards to other criminals for further illegal activities. Signs you have been a victim of card fraud could be that your card has been rejected when you try to make a payment, or you find transactions on your statements that you don't remember making.

To protect yourself from spear phishing:

1.Be sceptical: Even if the caller or email seems to know some details about you, remain sceptical. Legitimate organisations will not ask for sensitive information without proper verification.

2.Verify the request: If you receive a request for information or action, independently verify it through official channels. Use contact information obtained directly from the company's official website or customer service.

3.Watch for red flags: Look out for any unusual or unexpected requests, especially those that create urgency or pressure you to act quickly.

4.Secure personal Information: Limit the amount of personal information you share online and on social media platforms. Cybercriminals often gather details from public sources to use in their scams.

5.Use Two-Factor Authentication (2FA): Enable 2FA whenever possible to add an extra layer of security to your accounts, making it more difficult for unauthorised access.

6.Educate yourself and others: Stay informed about the latest phishing techniques and educate your colleagues, friends, and family about the risks and best practices for online security.

By staying vigilant, verifying requests, and maintaining a healthy scepticism, you can reduce the risk of falling victim to spear phishing attacks.

Beware of Phishing Scams

Smishing

This involves scams that entice individuals with extravagant prizes like expensive electronics, holidays, or cars often rely on the allure of unrealistically attractive offers. It is crucial to abide by the common adage, "If it sounds too good to be true, it probably is." Exercise caution and scepticism when encountering such offers, especially if they require personal information, payments, or other actions that seem unusual or too convenient. Verifying the legitimacy of such offers through reputable sources can help protect against falling victim to scams designed to exploit the desire for extraordinary rewards.

Vishing

Phone-based scams involve perpetrators posing as reputable companies to extract sensitive information such as personal details, bank card information, and passwords. It's important to be cautious when receiving unexpected calls, even if the caller claims to be from a trusted organisation. Legitimate companies typically do not request sensitive information over the phone without proper verification protocols.

To protect yourself from such scams:

1.Verify caller identity: Ask for the caller's name, company, and contact information. Independently verify their identity by using official contact details obtained directly from the company's website or customer service.

2.Avoid sharing personal information: Refrain from providing personal information, such as passwords or bank card details, over the phone unless you have initiated the call and are certain of the recipient's identity.

3.Be sceptical of urgency: Scammers often create a sense of urgency or fear to pressure individuals into sharing information quickly. Be sceptical of unexpected urgent calls.

4.Double-check requests: If the caller requests immediate action, such as making a payment or sharing sensitive information, double-check with the official company using verified contact information before proceeding.

5.Report suspicious calls: Report any suspicious calls to relevant authorities or the company the caller claims to represent. This helps prevent further attempts to scam others.

Remember, reputable organisations typically follow proper protocols and won't ask for sensitive information over the phone without proper verification. If in doubt, independently verify the legitimacy of the call before sharing any personal information.

Beware of Phishing Scams

Whaling

Whaling, also known as "CEO Fraud" or "Business Email Compromise (BEC)," is a form of targeted phishing that specifically focuses on high-profile individuals within an organisation, such as executives or senior managers. In a whaling attack, cybercriminals aim to impersonate a high-ranking colleague to trick employees into taking actions that could compromise sensitive information or lead to financial losses.

To safeguard against whaling attacks:

1.Implement strict verification protocols: Establish clear and rigorous procedures for verifying sensitive requests, especially those involving significant financial transactions. Encourage a culture of verification within the organisation.

2.Educate executives and employees: Provide specialised training to executives and employees about the risks and characteristics of whaling attacks. Emphasise the importance of scepticism and verification, even when receiving requests from seemingly trusted high-ranking colleagues.

3.Use multi-factor authentication (MFA): Enforce multi-factor authentication for email accounts and other critical systems to add an extra layer of security.

4.Strengthen email security: Implement advanced email security measures, including email filtering and monitoring systems, to identify and block phishing attempts.

5.Maintain up-to-date security policies: Regularly update security policies to address the evolving tactics used by cybercriminals. Keep employees informed about the latest threats and best practices.

6.Monitor financial transactions: Implement systems to monitor and scrutinise financial transactions, especially those initiated by email requests. Establish strict controls to validate and verify such transactions.

By incorporating these measures, businesses can enhance their defences against whaling attacks, reducing the risk of falling victim to schemes that exploit the trust placed in high-ranking individuals within the organisation.

Beware of Phishing Scams

Text fraud

Commonly known as SMS or text message fraud, is a form of scam where deceptive messages are sent to individuals with the aim of tricking them into providing sensitive information, making unauthorised transactions, or engaging in other malicious activities. This section will cover key aspects of text fraud, its common tactics, and preventive measures.

Common text fraud tactics:

1.Phishing texts: Fraudsters often send messages posing as legitimate entities such as banks, government agencies, or well-known companies. These texts typically contain urgent requests for personal information, account details, or payment.

2.Smishing (SMS phishing): Similar to phishing emails, smishing involves tricking individuals into clicking on malicious links or providing sensitive information through text messages. These messages may claim the recipient has won a prize, needs to update an account, or faces consequences if immediate action isn't taken.

3.Premium rate scams: Fraudsters may send texts promising enticing offers, free downloads, or exclusive content. Responding to these messages may unknowingly subscribe individuals to premium-rate services, resulting in unexpected charges on their phone bills.

4.Impersonation scams: Texts impersonating friends, family, or colleagues may request urgent financial assistance or sensitive information. Attackers exploit trust to deceive individuals into sharing confidential details.

By staying vigilant, verifying messages, and following security best practices, individuals can protect themselves from falling victim to text fraud and the associated risks.

Sim-swap fraud / sim card hijacking

In this attack, the criminal tries to convince your mobile operator that they are you, requesting a replacement SIM card for your phone number. Once they successfully convince the operator, they can take control of your mobile phone number.

This attack has serious implications because your mobile number is often used as a security measure for various accounts, including banking. With control of your phone number, the attacker can intercept calls and texts, potentially gaining access to two-factor authentication codes sent to your phone. This could lead to unauthorised access to your accounts, including sensitive information like online banking details.

To protect yourself from SIM swapping attacks, it's important to take security measures such as enabling additional authentication methods for your accounts, regularly monitoring your financial statements, and being cautious about sharing personal information, especially over the phone. Additionally, you can contact your mobile operator to inquire about additional security features or alerts they may offer to help prevent unauthorised SIM card changes.

Beware of Phishing Scams

Cont: Sim-swap fraud / sim card hijacking

Signs that you are a victim of a SIM swap attack:

1.If you find yourself unable to place calls, send texts, or access mobile data, it indicates a significant issue with your network connection. This could stem from a mere service outage, or it might be the result of a SIM card replacement, which could have inadvertently shifted your cell service and phone number to another user.

2.You receive notifications regarding activity occurring in another location.

3.The initial step for a SIM card hacker is often to restrict your access to accounts by altering passwords. Additionally, certain accounts may automatically enact access blocks as a security measure in response to numerous suspicious login attempts. Therefore, losing access serves as a clear indication that someone is actively compromising or attempting to compromise your accounts. In such cases, it is crucial to take immediate measures to enhance the security of your accounts.

4.The primary objective of a SIM swap attack is frequently to deplete the funds in a victim's bank account. If you receive notifications concerning transactions you did not initiate, it may be indicative of a SIM swapping incident. In such instances, besides contesting the unauthorised charges and fortifying your financial accounts, it is imperative to swiftly regain control of your phone number.

Steps to help protect yourself:

1.Avoid engaging with fraudulent emails, text messages, or phone calls. These methods are commonly employed by scammers seeking to obtain your personal information.

2.Exercise caution when sharing on social media. Refrain from posting personal details such as birthdates, pet names, and school information, as these details are commonly used as security questions for password resets.

3.In the event of your phone unexpectedly ceasing to function, it is advisable to promptly notify both your bank and mobile network for appropriate assistance.

4.Employ distinct and exclusive passwords that only you have knowledge of for enhanced security.

5.Ensure to modify your phone's default SIM PIN by manually establishing a PIN or password for your SIM through your phone's settings. Numerous carriers currently provide Number Transfer PINS, which activate when a SIM change is requested. This implies that in the event of a SIM swap attempt, the perpetrator will require your PIN first, regardless of any other details they may possess.

Greengage

For more info:

info@greengage.co

Painters' Hall,
9 Little Trinity Lane,
London EC4V 2AD UK

www.greengage.co