MPLP 5th Friday Webinar

January 2021

Security Hygiene for the New Year

Fifth Friday Webinar Series

Schedule for remainder of 2021:

- April 30, 2021
- July 30, 2021
- October 29, 2021

Recordings of and supporting materials for previous webinars available at:

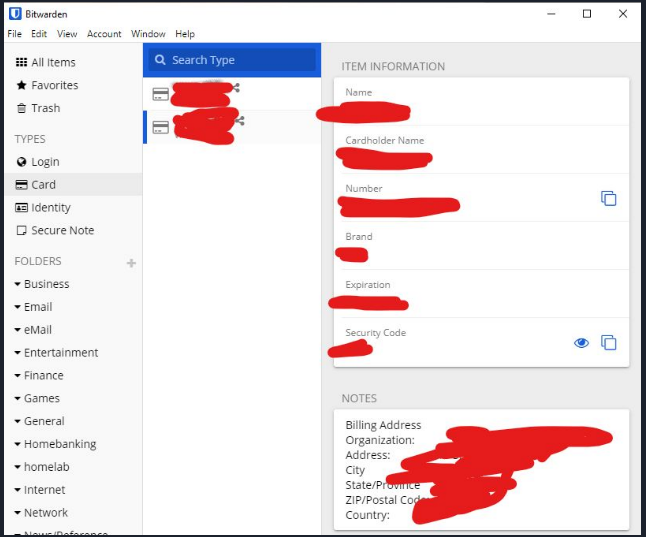
- http://www.mplp.org/Taskforces/technology

Agenda

- Passwords and Password Managers
- Multi-Factor Authentication
- Tools to Prevent Spam and Phishing
- Disabling Spammy Website Notifications
- Security Breach Policies
- Resources Available for Security Audits
- Q&A

Why Password Managers? (Bitwarden / Lastpass)

1. Lets you save website logins, field data, confidential inform, credit cards, MFA tokens, VPN settings, etc. It can also mask passwords and custom fields so they are not stolen by onlookers. Finally, you can create custom fields that you can copy with click.



[redacted]

ITEM INFORMATION

Name [redacted]

Cardholder Name [redacted]

Number [redacted]

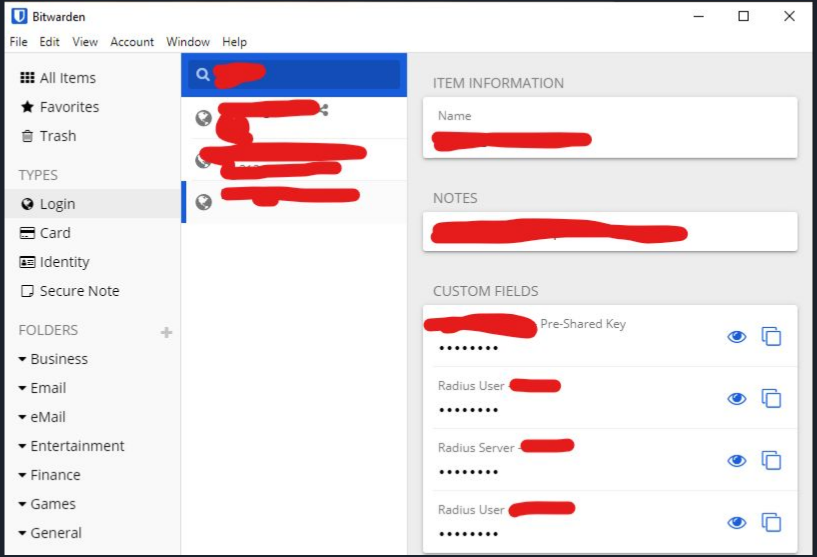
Brand [redacted]

Expiration [redacted]

Security Code [redacted]

NOTES

Billing Address
Organization:
Address:
City
State/Province
ZIP/Postal Code
Country: [redacted]



[redacted]

ITEM INFORMATION

Name [redacted]

NOTES

[redacted]

CUSTOM FIELDS

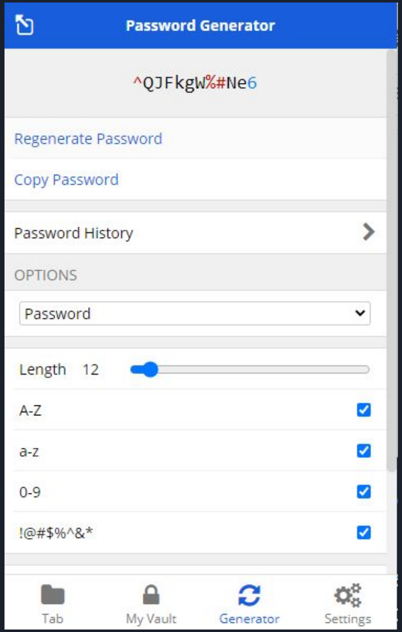
[redacted] Pre-Shared Key
••••••••

Radius User [redacted]
••••••••

Radius Server [redacted]
••••••••

Radius User [redacted]
••••••••

2. **The Master Password:** The main purpose of using a password manager is so you can generate ****unique**** passwords with the appropriate level of complexity for every website account you use. This can be done in both a browser extension for Chrome, Edge, and Firefox, or with a native app in Windows, MacOS and Linux. This makes it easy to meet differing website password standards. It also makes it easy to create unique passwords for all of your sites and eliminate the need to remember passwords through use of a single, complex password that you can remember.



Password Generator

^QJFkgW%#Ne6

Password

Length 12

A-Z ☑

a-z ☑

0-9 ☑

!@#$%^&* ☑

More Features of Bitwarden/Lastpass

3. Import passwords from: LastPass, 1Password, Firefox and Chrome.
4. Secure your password vault with MFA so even if someone hacks your email account they will not get your passwords.
5. Access passwords and confidential information from your cell phone that is secured by fingerprint ID.
6. Share collections among multiple users based on customizable permission groups with paid Team account.
7. Team Sharing using affordable, paid versions of Bitwarden and Lastpass.

Team sharing in Bitwarden is half the price of Lastpass and has most if not all of the same features.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA; encompassing Two-factor authentication or 2FA, along with similar terms) is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors)

Google - 2-Step Verification

How it works

1. Whenever you sign in to Google, you'll enter your password as usual (to protect your account with something you know)
2. Then, a code will be sent to your phone via text, voice call, or our mobile app. Or, if you have a Security Key, you can insert it into your computer’s USB port (to protect your account with something you have: your phone or Security Key).

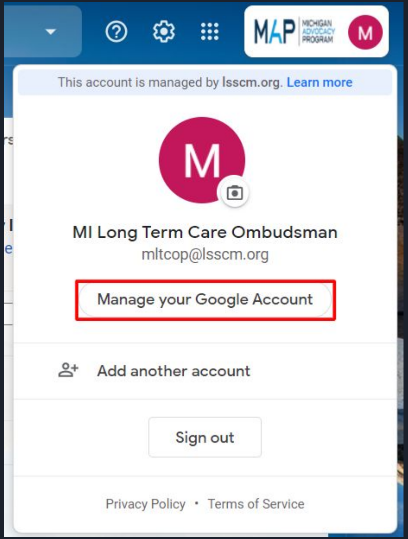
Note: During sign-in, you can choose NOT to use 2-Step Verification again on that particular computer. From then on, that computer will only ask for your password when you sign in.

Turn on Google 2-Step Verification

Open your Google Account.

In the navigation panel, select Security.

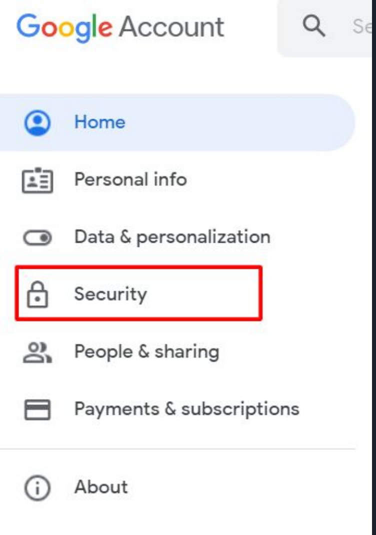
Under “Signing in to Google,” select 2-Step Verification and then Get started.

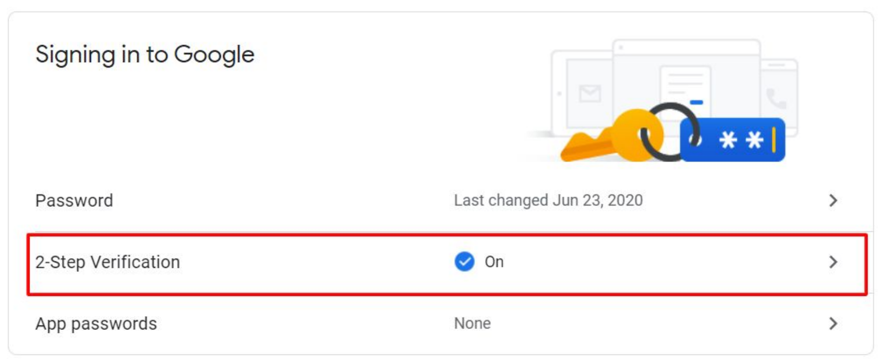


This account is managed by lsscm.org. Learn more

MI Long Term Care Ombudsman
mltcop@lsscm.org

MAP MICHIGAN ADVOCACY PROGRAM
M
Manage your Google Account
Add another account
Sign out
Privacy Policy • Terms of Service

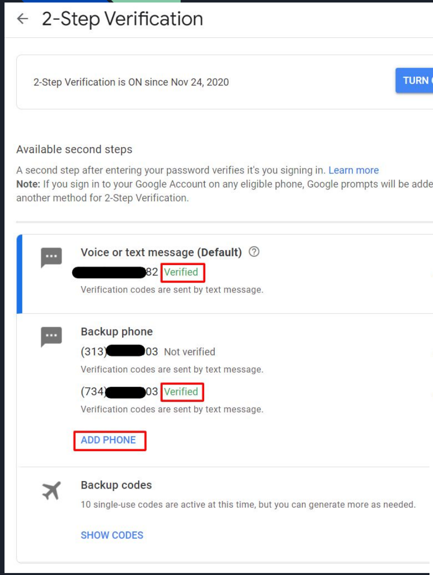




Signing in to Google

Password	Last changed Jun 23, 2020
2-Step Verification	✓ On
App passwords	None

Turn on Google 2-Step Verification - Continued



← 2-Step Verification

2-Step Verification is ON since Nov 24, 2020 TURN OFF

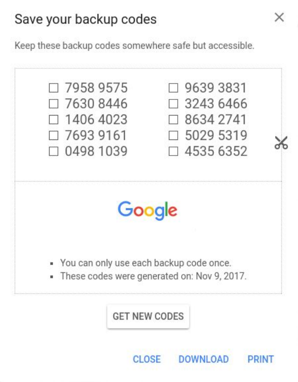
Available second steps

A second step after entering your password verifies it's you signing in. Learn more
Note: If you sign in to your Google Account on any eligible phone, Google prompts will be added as another method for 2-Step Verification.

Voice or text message (Default)
[redacted]82 Verified
Verification codes are sent by text message.

Backup phone
(313)[redacted]03 Not verified
Verification codes are sent by text message.
(734)[redacted]03 Verified
Verification codes are sent by text message.
ADD PHONE

Backup codes
10 single-use codes are active at this time, but you can generate more as needed.
SHOW CODES



Save your backup codes

Keep these backup codes somewhere safe but accessible.

☐ 7958 9575
☐ 7630 8446
☐ 1406 4023
☐ 7693 9161
☐ 0498 1039

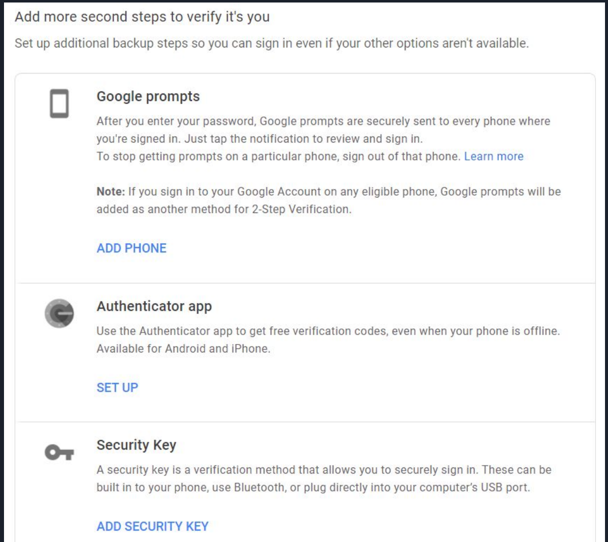
☐ 9639 3831
☐ 3243 6466
☐ 8634 2741
☐ 5029 5319
☐ 4535 6352

Google

- You can only use each backup code once.
- These codes were generated on: Nov 9, 2017.

GET NEW CODES

CLOSE DOWNLOAD PRINT



Add more second steps to verify it's you

Set up additional backup steps so you can sign in even if your other options aren't available.

Google prompts
After you enter your password, Google prompts are securely sent to every phone where you're signed in. Just tap the notification to review and sign in.
To stop getting prompts on a particular phone, sign out of that phone. Learn more

Note: If you sign in to your Google Account on any eligible phone, Google prompts will be added as another method for 2-Step Verification.

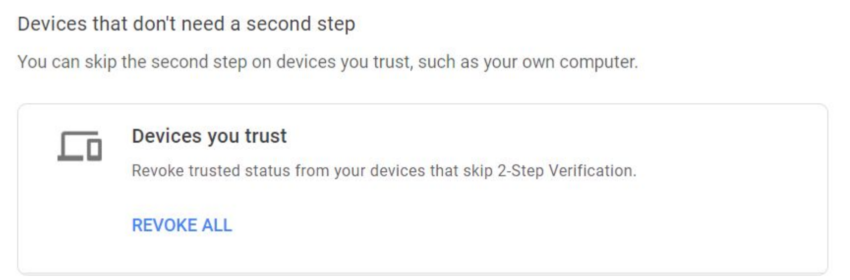
ADD PHONE

Authenticator app
Use the Authenticator app to get free verification codes, even when your phone is offline. Available for Android and iPhone.

SET UP

Security Key
A security key is a verification method that allows you to securely sign in. These can be built in to your phone, use Bluetooth, or plug directly into your computer's USB port.

ADD SECURITY KEY



Devices that don't need a second step

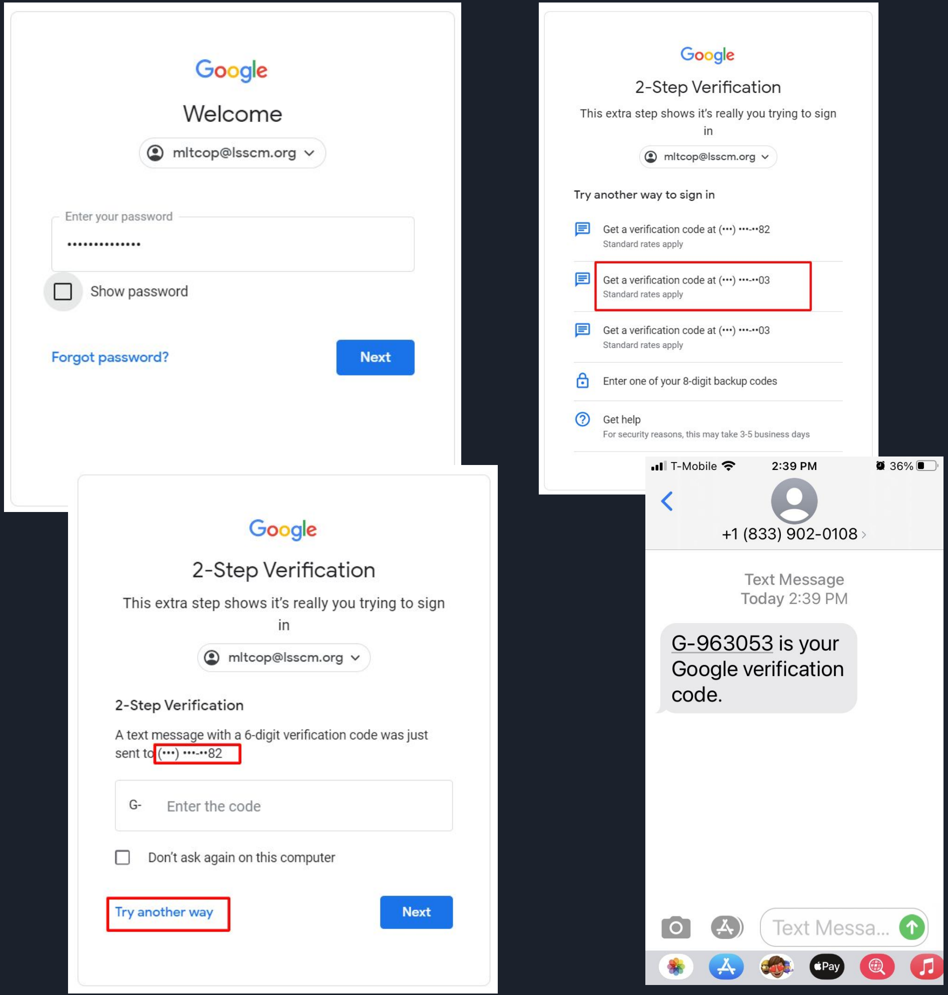
You can skip the second step on devices you trust, such as your own computer.

Devices you trust
Revoke trusted status from your devices that skip 2-Step Verification.

REVOKE ALL

Google 2-Step Verification via a text message

If you set up multiple phone numbers for verification, you can select ‘Try another way’ to select a phone number you want to use at the time of login.



Google

Welcome

mltcop@lsscm.org

Enter your password

••••••••••••••

□ Show password

Forgot password?

Next

Google

2-Step Verification

This extra step shows it’s really you trying to sign in

mltcop@lsscm.org

2-Step Verification

A text message with a 6-digit verification code was just sent to (•••) •••-••82

G- Enter the code

□ Don’t ask again on this computer

Try another way

Next

Google

2-Step Verification

This extra step shows it’s really you trying to sign in

mltcop@lsscm.org

Try another way to sign in

Get a verification code at (•••) •••-••82
Standard rates apply

Get a verification code at (•••) •••-••03
Standard rates apply

Get a verification code at (•••) •••-••03
Standard rates apply

Enter one of your 8-digit backup codes

Get help
For security reasons, this may take 3-5 business days

T-Mobile 2:39 PM 36%

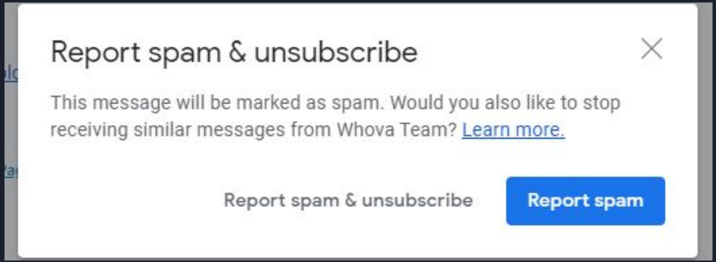
+1 (833) 902-0108

Text Message
Today 2:39 PM

G-963053 is your Google verification code.

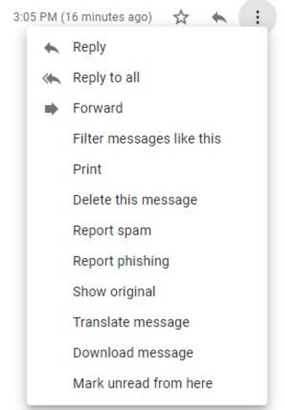
Text Messa...

Spam & Phishing – Definitions and Gmail



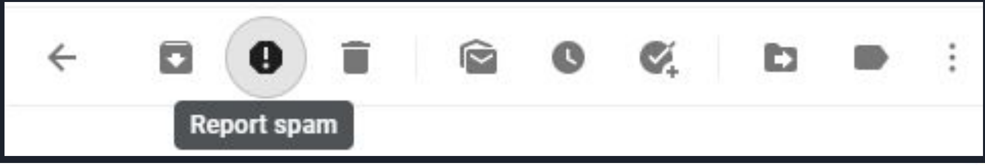
Report spam & unsubscribe

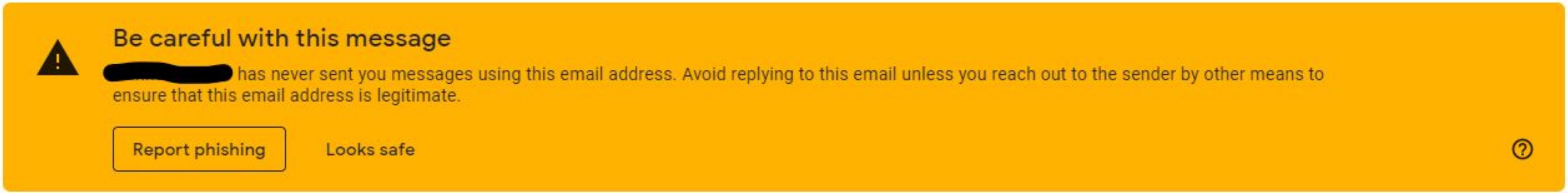
This message will be marked as spam. Would you also like to stop receiving similar messages from Whova Team? Learn more.



3:05 PM (16 minutes ago)

- Spam: "junk" email; not specific; usually some kind of ad or "deal"
- Phishing: more targeted; usually purports to be some sort of reputable organization; will request financial/personal information
- Spear-phishing: will come from a **known contact**; won't look like "typical" spam; will almost always be attempting to procure a username/password
- If you believe you have been subjected to an attack, **please** don't hesitate to email map-it@lsscm.org
- No need to live in fear; just always have the question "Was I expecting to get this?" in the back of your mind
- In 99.99% of cases, simply **opening** an email will **not** do any harm



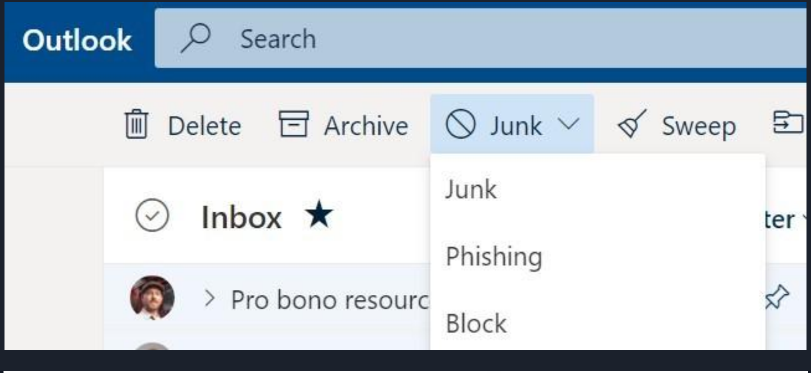


Be careful with this message

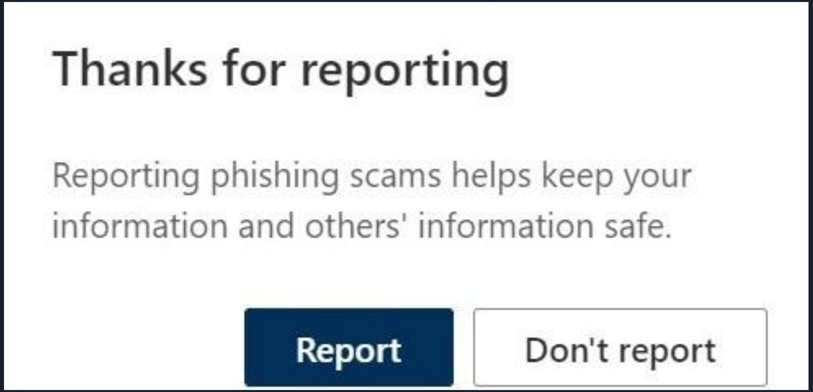
[redacted] has never sent you messages using this email address. Avoid replying to this email unless you reach out to the sender by other means to ensure that this email address is legitimate.

Spam & Phishing Emails in Outlook.com

To report a spam email, click on Junk>Junk. To report a phishing email, click on Junk>Phishing.



After marking an email as a junk or phishing email, you have the option to report the email, which results in a copy of the email being sent to Microsoft for analysis to help improve their filters.



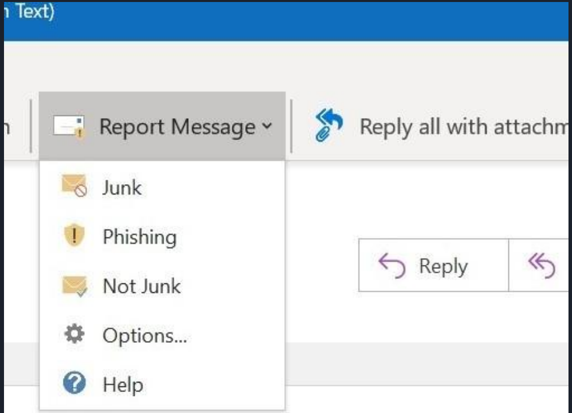
Thanks for reporting

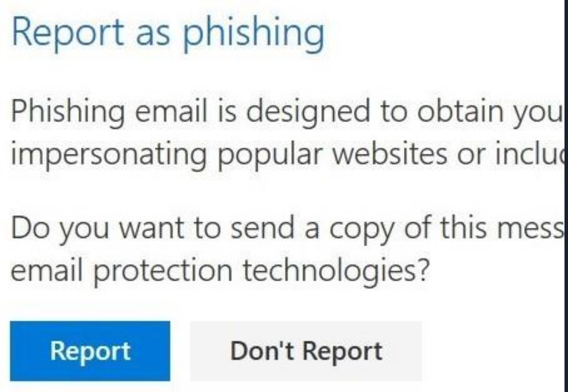
Reporting phishing scams helps keep your information and others' information safe.

Spam & Phishing Emails in Outlook 365 Desktop

You can use the Report Message add-in for Outlook. Once installed, to report a junk email, click on Report Message>Junk. To report a phishing email, click on Report Message>Phishing.

After marking an email as a junk or phishing email, you have the option to report the email, which results in a copy of the email being sent to Microsoft for analysis to help improve their filters.




Report as phishing

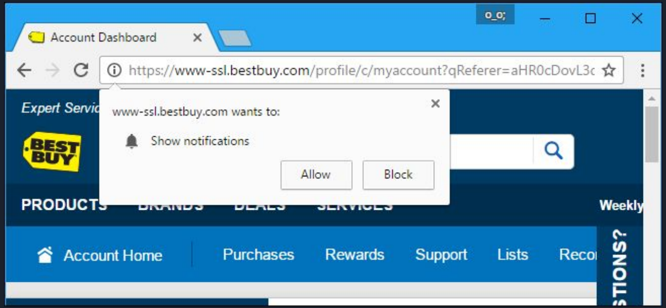
Phishing email is designed to obtain you
impersonating popular websites or incluc

Do you want to send a copy of this mess
email protection technologies?

Disable Website notifications in Chrome, Edge and Firefox to prevent spam notifications

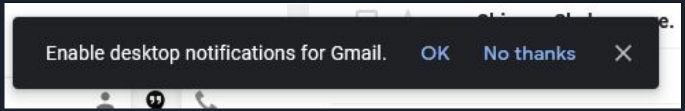
Today’s browsers allow websites to show you notifications in the background if you give them permission. You will often see these on popular web apps like Gmail, news and shopping websites. You can disable these notification, but in many cases they are useful.

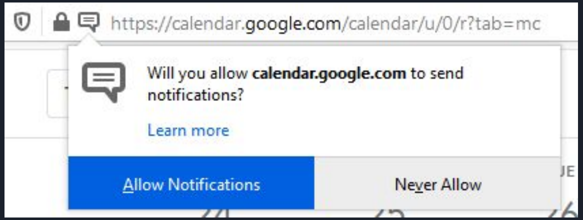
Unfortunately, website notifications have become a popular spam promotion method for nefarious sites. For example, a user might get a notification that their device isn’t secure and that you should install a malicious app to clean your “infected” computer.


https://www-ssl.bestbuy.com/profile/c/myaccount?qReferer=aHR0cDovL3c

www-ssl.bestbuy.com wants to:

Show notifications


Enable desktop notifications for Gmail.

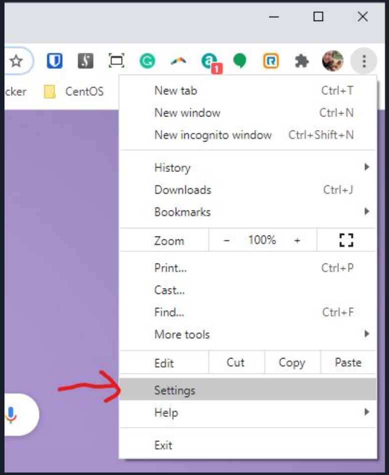

https://calendar.google.com/calendar/u/0/r?tab=mc

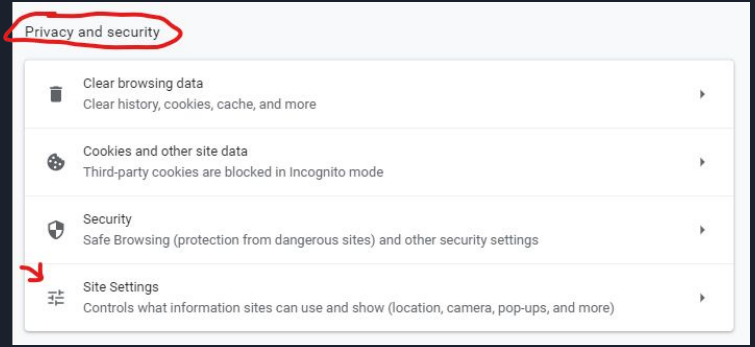
Will you allow **calendar.google.com** to send notifications?

Disable a notification in Chrome and Edge

To disable spam notifications in Chrome and Edge, click the menu button in the upper right corner of the browser and select “Settings”.

1. Click the “Site Settings” under the Privacy and security section.




Privacy and security

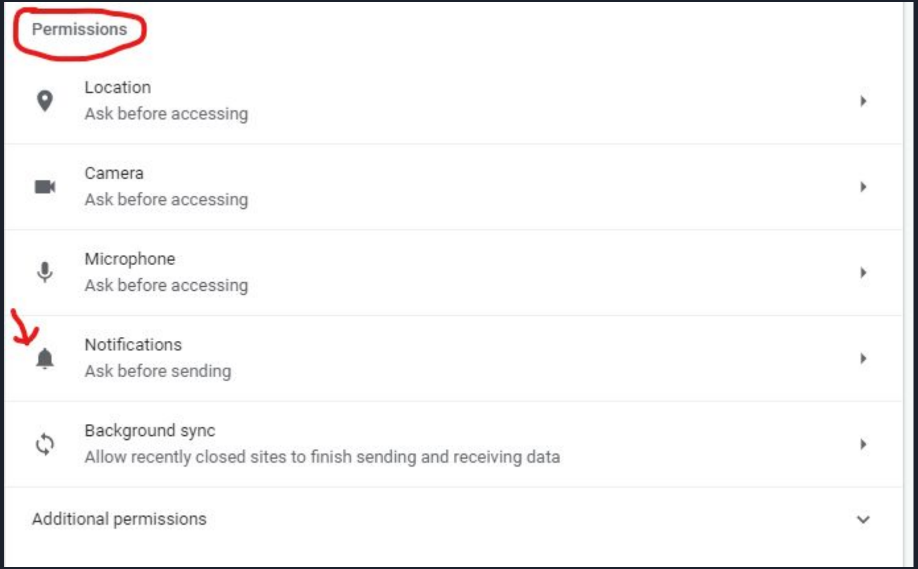
Clear browsing data
Clear history, cookies, cache, and more

Cookies and other site data
Third-party cookies are blocked in Incognito mode

Security
Safe Browsing (protection from dangerous sites) and other security settings

Site Settings
Controls what information sites can use and show (location, camera, pop-ups, and more)

2. Click “Notifcations” under the Permissions section. Here you will see all of the sites that you’ve given permission to send notifications to your computer. You will probably see things you want to keep (gmail, facebook, etc.) and ones you don’t recognize. It is safe to remove the ones you don’t recognize. The next time you visit the site it will prompt you again for permission to post the notification.



Permissions

Location
Ask before accessing

Camera
Ask before accessing

Microphone
Ask before accessing

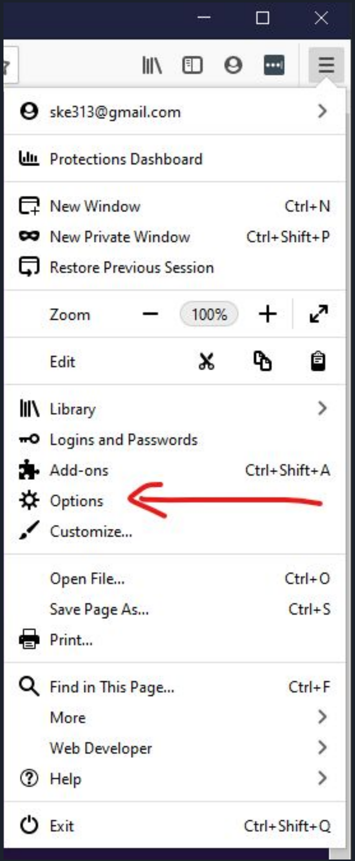
Notifications
Ask before sending

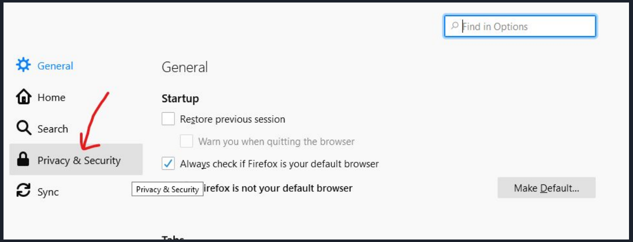
Background sync
Allow recently closed sites to finish sending and receiving data

Additional permissions

Disable Website Notification in Firefox

1. To disable a spammy notification in Firefox, click the “Options” link in the hamburger menu on the upper right corner of the browser.
2. Click the Privacy and Security button on the menu on the top left of the Options screen.
3. Click the Settings button next to Notifications in the Permissions section
4. Allow, Block or Remove websites from the list.



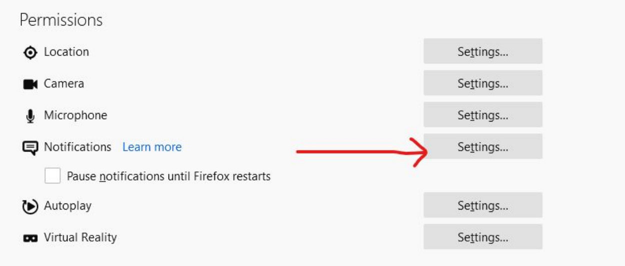


□ Restore previous session

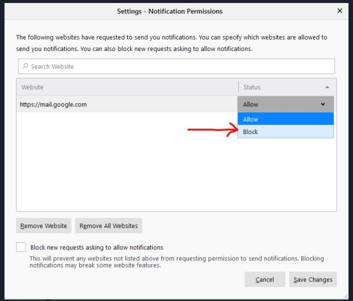
□ Warn you when quitting the browser

☑ Always check if Firefox is your default browser

irefox is not your default browser



□ Pause notifications until Firefox restarts



The following websites have requested to send you notifications. You can specify which websites are allowed to send you notifications. You can also block new requests asking to allow notifications.

Website	Status
https://mail.google.com	Allow

□ Block new requests asking to allow notifications

This will prevent any websites not listed above from requesting permission to send notifications. Blocking notifications may break some website features.

Security Breach Policies - MAP Sample

Response to Data Breach

A. Definitions.

1. “Data Breach” means the loss of control, compromise, authorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user access or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purposes.

2. “Personally Identifying Information (PII)” means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

B. Actions in the event of a data breach.

MAP stores personally identifiable information in staff email (currently Gmail), in our case management system (currently Pika), and in our document storage system (currently Office 365/SharePoint). In the event of an actual or imminent breach of personally identifiable information, MAP IT staff will take all reasonable measures to immediately stop and repair the actual or imminent breach.

C. Notifications in the event of a data breach.

1. In the event of a data breach, MAP will:
    a. notify the affected individual(s) without unreasonable delay, consistent with legitimate needs of law enforcement, or consistent with measures necessary to determine the scope of the breach and to restore the integrity of the data system;
    b. notify law enforcement of the breach as appropriate; and
    c. notify funders as required by the terms and conditions of the funding source.

2. MAP will include the following information when notifying the affected individual(s):

    a. That the individual's personal information was acquired or reasonably believed to be acquired by an unauthorized person;

    b. The date or dates of the breach or possible breach;

    c. Those elements of personal information that were likely acquired.

3. MAP may delay notification if a law enforcement agency requests a delay for criminal investigation purposes. Notification will be made after the law enforcement agency determines that it will not impede the investigation.

4. MAP will notify the affected individual(s) by one of the following methods:

    a. Written notice to the person's last known address in MAP's records;

    b. Electronic notice consistent with applicable provisions of 15 U.S.C. 7001;

    c. Telephonic notice to the last known telephone number in MAP's records; or

    d. Substitute notice, such as electronic mail, prominent posting on https://miadvocacy.org, or notification to applicable local or statewide media, if one of the following conditions exist:

        i. the cost of providing notice would exceed $250,000

        ii. the number of individuals to be notified exceeds 500,000; or

        iii. MAP has insufficient contact information.

Resources for Security Policies and Audits

LSNTAP.org:

- Improving Security webinar from March 2018
- Becoming a CyberSecurity Ninja series from 2017
- Information Security toolkit for Legal Aid programs from 2018
- Many more to come in the future!

SANS Institute: https://www.sans.org/information-security-policy/

Do you have resources to share?

What resources would you like to see shared on LSNTAP? What do you need?

Thank you!

We are:

Angela Tripp, Director MLH, Co-Director MSAS, and Co-Manager of MPLP (focusing on IT); trippa@mplp.org, 734-714-3242

Scott Ellis, IT Systems Administrator, MPLP; scoellis@mplp.org, 734-714-3234

Wilson Suprapto, Statewide Web Developer, MPLP; wsuprapto@mplp.org, 734- 998-6100 Ext. 618

Matt Olgren, Administrative Assistant/Desktop Support, MAP; molgren@lsscm.org, 734-998-6100 ext. 145

And guest starring:

Jason O’Brien, Director of Program Operations, LAWM; jtobrien@lawestmi.org, 616-608-8040