

To Whom It May Concern,

On behalf of School of Food, a Humanim Social Enterprise, we are writing to inform you of a security breach incident that occurred on the [School of Food website](#) on March 11, 2024. Pursuant to the Maryland Personal Information Protection Act (PIPA), we are required to notify the Office of the Attorney General regarding this breach.

Nature of the Security Breach: Our server's automated malware scanner detected malware on the schooloffood account, triggering an immediate alert on March 11, 2024. We took prompt action to eliminate the threat on the same day and restored the website to its full functionality.

Information Compromised: As a result of this breach, all user account information stored on our website should be considered compromised. This includes usernames, email addresses, first and last names, and encrypted passwords.

Number of Maryland Residents Being Notified: 36,401 accounts are being notified about this breach. It is important to note that this figure includes both legitimate user accounts and potentially fake accounts or bots. Attached please find the list.

Steps Taken to Restore Integrity of the System: In response to this breach, we have taken the following steps to restore the integrity of our system:

1. Conducted a thorough investigation into the incident to understand the extent of the breach and identify potential vulnerabilities.
2. Implemented additional security measures to prevent similar incidents from occurring in the future, including enhancing our malware detection and removal protocols.
3. Reviewed and updated our data protection policies and procedures to ensure compliance with relevant regulations and best practices.
4. Provided guidance and support to affected users on how to secure their accounts and mitigate any potential risks associated with the breach.

Attached please find a copy of the notification that is being sent to affected consumers for your reference.

We understand the seriousness of this matter and are committed to ensuring the security and privacy of our users' information. Should you require any further information or assistance regarding this incident, please do not hesitate to contact us at 410.381.7171 or via email at dellis@humanim.org or communications@humanim.org.

Can you please confirm the receipt of this email? Thank you!

Sincerely,

Diana Ellis
Vice President of Strategic Partnerships and Development

HUMANIM

dellis@humanim.org

www.humanim.org

Connect with us on social media!

[Facebook](#) . [Twitter](#) . [Instagram](#) . [LinkedIn](#)

Humanim, Inc. is a not-for-profit, 501(c)(3), organization.

Confidentiality Statement:

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. Please notify the sender immediately if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the named addressee you should not disseminate, distribute or copy this e-mail.

Subject: Important Notice Regarding Security Breach at School of Food Website

Dear _____

We are writing to inform you of a recent security incident that has occurred on our [School of Food](#) website, potentially impacting the security of your personal information. Protecting your data is of utmost importance to us, and we are taking this matter very seriously.

Our investigation has revealed that unauthorized access was gained to our School of Food website on March 11, 2024, compromising personal information. This data includes usernames, email addresses, first and last names, and encrypted passwords. We want to stress the fact that the passwords in the database were one-way-encrypted and randomly salted. This means that the password information that may have been extracted are not usable passwords by themselves, but they could potentially be used to figure out what these user passwords are in time.

We want to assure you that upon discovery of this breach, immediate action was taken by our team, the security threat has been removed and the website is fully functioning in.

Given the nature of the breach, we recommend changing any reused password immediately. Choose a strong, unique password that you do not use for any other accounts.

If you have any questions or concerns regarding this incident, please do not hesitate to contact us. You can reach our team at communications@humanim.org or 410-381-7171.

In addition to contacting us, we recommend that you contact credit reporting agencies to protect your identity:

1. Equifax: Toll-free number: 1-888-378-4329 Email Address: customerservice.eportsupport@equifax.com
2. Experian: Toll-free number: 1-888-397-3742
3. TransUnion: Toll-free number: 1-800-916-8800 Email Address: clientsupport@transunion.com

Contact Information for Federal Trade Commission (FTC) and Maryland Office of the Attorney General (OAG): You can also obtain further information and guidance on steps to prevent identity theft from the following authorities:

1. Federal Trade Commission (FTC): Toll-free number: 1-877-FTC-HELP Website: www.ftc.org
2. Maryland Office of the Attorney General (OAG): Toll-free number: 1-888-743-0023 Website: www.marylandattorneygeneral.gov

We apologize for any inconvenience this may cause and assure you that we are taking every necessary measure to prevent such incidents in the future. Your trust is paramount to us, and we are committed to ensuring the security of your information.

Thank you for your understanding and cooperation.

Sincerely,

Humanim Communications Department