



Hello,

I'm writing to report a data breach on the website for the [Alpha Workshop for Young Writers](#), a small non-profit based in Pittsburgh, PA.



The number of Maryland residents being notified

2

What occurred:

An unknown person compromised an existing user's admin credentials to log into the backend of the website (i.e. into WordPress). They placed malware and phishing software into the website code. and other 'spammy' links to inappropriate websites.

Timeline of breach:

The data breach occurred on March 20, 2022 at approximately 10:29:32 PM ET (afternoon of 21st March in Eastern Australia, our webmaster's time zone). An unknown person logged in using the previous developer's user name (JeremyT) and password.

The webmaster was notified by email by Wordfence, our security plugin software on the website, that this user "JeremyT" had logged in from Russia. Because this seemed unlikely--we have no volunteers in Russia--the webmaster emailed Jeremiah Tolbert, the previous developer to query if/why he was logging into the website. He responded that he had not logged in.

Due to the time zone difference with Eastern Australia, the webmaster had retired for the night before receiving Jeremiah's response.

How the person compromised the login is unknown. The site is protected against brute force attacks (repeated attempts).

The breach was quickly resolved, within about 30 hours. The majority of the time was 'overnight' due to time zones. Afterward, all users were required to change their password, and we added two-factor authentication to all admin accounts.

Information they accessed:

For 2022 workshop applicants the following information was accessible to the unauthorized user:

- Applicant and parent/guardian names
- birthdate
- email addresses for applicants and parents
- home address
- COVID-19 vaccination status (yes/no)
- racial identification
- family income bracket
- user IP address
- general non-personally identifiable application information such as essays, financial aid requests, and submission stories.

A sample of our notification letter is attached. Please confirm receipt so we can send it out as soon as possible.

Best,



Alpha Workshop for Young Writers

Alpha Workshop For Young Writers Inc.
PO Box 7770
Pittsburgh, PA 15215

April ___, 2022

NOTICE OF DATA BREACH

Dear Alpha Workshop For Young Writers Inc. applicant:

On behalf of Alpha Workshop For Young Writers Inc. ("Alpha") we are writing to inform you of a recent security incident where an unauthorized actor may have accessed your Alpha 2022 workshop application information. While we have no evidence to suggest that your information has been misused, we are notifying potentially affected individuals.

What Happened? Alpha workshop applicants apply through an online application process. On March 20, 2022, we learned that an unauthorized actor had launched an attack on our website backend. Our webmaster was immediately notified via our security plugin software, immediately began an investigation, and then took prompt action to prevent any further unauthorized access to this information.

Based on our investigation, it appears an unauthorized user accessed the backend of our website to place malware and phishing software into our code and include other "spam" links to websites. Our webmaster worked to investigate the situation to ensure the user login was not legitimate and the attack lasted only approximately thirty (30) hours. The administrators of the website have taken steps to increase the security of their logins and prevent future attacks, and Alpha has security awareness software still in place. During the attack, the unauthorized user was able to access our 2022 workshop applications stored on the site.

What Information Was Involved? For 2022 workshop applicants the following information was accessible to the unauthorized user: Applicant and parent/guardian names, birthdate, email addresses for applicants and parents, home address, vaccination status (yes/no), racial identification, family income bracket, user IP address, and general non-personally identifiable application information such as essays, financial aid requests, etc.

The types of personal information that most commonly lead to identity theft issues were not stored on the site. No driver's license, state identification card, social security number, credit card, debit card, banking, or other payment login, account login, or passport information was accessible. No information relating to minors aged 13 years or under was included.

What We Are Doing. We immediately stopped the unauthorized access once we confirmed the login was unauthorized. We have increased our login security on our website and are notifying those affected.

What You Can Do. While we currently have no evidence indicating that your personal information has been fraudulently used as a result of this incident, you can take steps to further reduce the risk of potential fraud, including by reviewing personal accounts statements and credit reports. While password information was not included in the breach, it is also recommended you change your passwords, especially those associated with your email address.

Other Important Information. Out of an abundance of caution we are also providing you the following information about steps consumers can take as a general best practices to protect against potential misuse of information:

Remain vigilant for incidents of potential fraud and identity theft, including by regularly reviewing your account statements and monitoring your credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud or anything you do not understand, please call your financial institution(s).

In addition, if you believe there has been an issue of identify theft, for any reason or cause, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, contact the FTC by visiting www.ftc.gov/idtheft, calling 877-438-4338, or writing to the FTC's Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. If you file a police report for identity theft, you should obtain a copy of such report as you may need to give copies of the report to others to remedy any fraudulent activity.

It's also helpful to know you may also periodically obtain a free copy of your credit report from each nationwide credit reporting agency ("CRA"). If you discover information on your credit report arising from a fraudulent transaction, you should request that the CRA delete that information from your credit report file. You are entitled to one free copy of your credit report every 12 months from each of the three CRAs. You may obtain a copy of your credit report by visiting www.annualcreditreport.com or by calling 1-877-322-8228. You may contact the CRAs at:

Equifax (www.equifax.com)
General Contact:
P.O. Box 740241, Atlanta, GA 30374
800-685-1111
Fraud Alerts and Security Freezes:
P.O. Box 740256, Atlanta, GA 30374

Experian
(www.experian.com)
General Contact:
P.O. Box 2104, Allen, TX 75013
888-397-3742
Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
General Contact, Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
800-916-8800

You can also contact each of the CRAs at the numbers listed above to place a security freeze at no cost to restrict access to your credit report. You will need to supply your name, address, date of birth, Social Security number, and other personal information. After receiving your request, each CRA will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

Again, no financial, payment, or other login information was accessed, we are simply providing you this information as an additional precaution.

State Specific Information:

For Maryland residents: The Attorney General can be contacted at Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

For New York residents: The Attorney General can be contacted at 120 Broadway, 3rd Floor New York, NY 10271, Fax: 212-416-6003, breach.security@ag.ny.gov

For North Carolina residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699, 919-716-6400, www.ncdoj.gov.

For all other residents: Information on how to contact your state attorney general may be found at www.naag.org/naag/attorneys-general/whos-my-ag.php.

For More Information. For more information about this incident, or if you have questions or concerns, you may contact us at _____ (phone) or _____(email) or via the address above.

Sincerely,

Patrick Ropp
Board President
Alpha Workshop For Young Writers Inc.

