Subject: Important Security Update: Protecting Your Accounts and Email Safety. (6th Nov 2026)

Member's emails have recently been compromised so we would like to share an important note regarding cybersecurity. Targeted hacking attempts were made at personal email addresses where attackers attempted an extortion scam using old passwords. Fortunately, no harm was done, but it was a jarring experience that prompted us to re-evaluate our online security.

NB. For peace of mind, use the below website, inserting your email address, to check if it's been compromised. If it has, 'don't panic', just change it to a more secure address. https://haveibeenpwned.com/.

We want to make sure everyone in our community stays safe.

If you are using an older ISP-provided email address (such as TalkTalk, BT, Virgin Media, etc., I strongly encourage you to evaluate your security settings. Many older legacy email platforms do not feature the robust, modern spam-filtering and advanced multi-factor security protections that modern dedicated platforms provide.

Here are some steps everyone should consider taking as soon as possible:

Consider Migrating to a Dedicated Provider: If you are using an older internet service provider email, consider switching to a highly secure, modern platform like Gmail or Proton Mail. (See more below) They have world-class security infrastructures to block these threats before they reach you.

Never Reuse Passwords: If a hacker gets a hold of one password you used on an old forum or shopping site, they will try to use it to unlock your email and banking. Every account needs a completely unique password.

Turn on Two-Factor Authentication (2FA): Enable 2FA on your email and all critical accounts. This ensures that even if a hacker knows your password, they cannot log in without a code sent to your phone or authenticator app.

Don't Panic over Extortion Emails: If you ever receive an email from a "hacker" claiming they have your password and demanding money, do not pay them. They are almost always using old, leaked data to scare you. Simply change your passwords immediately.

Crucial Next Steps For You - Gmail as an example:

If you have already set up a Gmail account, or another secure account, make sure to complete these security clean-up steps:

Update your critical logins: Change the registered email address on your banking, PayPal, social media, and domain/website hosting accounts, as well as your Dentist, Doctor's surgery, Hospital from your old email address to your new 'Gmail address'.

Painstaking work but well worth doing, because a great deal of your personal date such as your home address, tel. number, etc. is often included in such emails to you.

Secure the Gmail: Make sure you immediately go into your Google Account settings and turn on 2-Step Verification (2FA) so your new home base is completely locked down.

Audit your site: Ensure that your website's administrative back end (WordPress, admin panel, etc.) is no longer tied to the compromised email address.

Hopefully, sharing this recent experience will likely save several of our members from falling victim to similar scams.

Stay safe out there, and let's keep our community secure!