**Friends of Smithgall Woods**

**Website Security Recommendations**

1. Backup website (already done).
2. Remove all unnecessary accounts, then change remaining account passwords
   1. Hosting site
      1. 17505820 – Dr. Huber’s account
   2. Databases
      1. [db357026991](https://my.1and1.com/mysql-database-details/db357026991?__lf=ftp_create_account_flow) (FSGW)
      2. [db358933030](https://my.1and1.com/mysql-database-details/db358933030?__lf=ftp_create_account_flow) (FSGWData)
      3. [db360322876](https://my.1and1.com/mysql-database-details/db360322876?__lf=ftp_create_account_flow) (Fresh root WP install) – This is the database the WordPress site pulls from and saves to for page content.
      4. [db265662256](https://my.1and1.com/mysql-database-details/db265662256?__lf=ftp_create_account_flow) (login and hours database) – I think this is the volunteer hours db.
      5. [db268336715](https://my.1and1.com/mysql-database-details/db268336715?__lf=ftp_create_account_flow) (calendardb)
   3. FTP accounts
      1. [u48922589](https://my.1and1.com/ftp-account-details/54939311?__lf=ftp_create_account_flow)
      2. [u48922589-drdan](https://my.1and1.com/ftp-account-details/75464305?__lf=ftp_create_account_flow) – This is the only account we can access. The passwords for the others are incorrect. We only need one account, so I think we should get rid of the rest.
      3. [u48922589-students](https://my.1and1.com/ftp-account-details/76946453?__lf=ftp_create_account_flow)
      4. [u48922589-Admin](https://my.1and1.com/ftp-account-details/77483152?__lf=ftp_create_account_flow)
   4. WordPress accounts
      1. mhuber ([mhuber@uga.edu](mailto:mhuber@uga.edu))
      2. admin ([youdomaincom977@gmail.com](mailto:youdomaincom977@gmail.com)) – This is the default admin name in WP and should be changed via the wp\_users table in the database, if it doesn’t break anything.
      3. Admin1 ([webmaster@friendsofsmithgallwoods.org](mailto:webmaster@friendsofsmithgallwoods.org))
      4. lcompton ([compton.pl@gmail.com](mailto:compton.pl@gmail.com)) – Who is Larry Compton?
3. Find and remove bad code.
   1. If code cannot be found, the site will need to be rebuilt. We will develop a plan for that if needed.
4. Update all website software.
   1. WordPress
   2. PHP – Should be running on PHP 7.0, but are currently on 5.2.
   3. WordPress theme
   4. WordPress plugins
      1. Akismet
      2. NextGEN Gallery
      3. Page Links To
      4. Seo Meta Tags
5. 1&1 security features
   1. 1&1 SiteLock - <https://help.1and1.com/hosting-c37630/sitelock-c85170/what-is-1and1-sitelock-a792625.html>
      1. Basic ($.99/month)
         1. Daily malware scan
         2. Trust Seal
         3. Search engine blacklist monitoring
         4. SSL verification
         5. Web app scan (on demand once a month)
         6. SQL injection scan (on demand once a month)
         7. XSS scan (on demand once a month)
         8. Number of pages monitored – 25
      2. Premium ($4.99/month)
         1. Daily malware scan
         2. Trust Seal
         3. Search engine blacklist monitoring
         4. SSL verification
         5. Web app scan
         6. SQL injection scan
         7. XSS scan
         8. File Change Monitoring
         9. Number of pages monitored – 500

We need to contact Dr. Huber with our recommendations so we can get approval from him and the Friends of Smithgall Woods. I can create a revised version of this document for them to review.

To implement the plan, the site may need to be down for a period of time. The length of time will probably be no more than a few hours if the bad code can be found, because the password changes and software updates should not take long to do. However, if the site has to be rebuilt, it will be down longer. To calculate the time required for that, we would have to develop a rebuild plan, which I can do.

As a side note, I believe it’s important to determine that Dr. Huber’s computer(s) are secure, since there’s a strong likelihood that the site credentials were stolen from him or someone else, perhaps by a keylogger installed on his computer. Until he is sure that his computers are secure, we don’t want him logging into the website with new passwords, or we’ll be right back where we started.