HOME CYBER DEFENSE

ARE YOU SAFE FROM CYBER CRIME?

WEEKLY

Volume #4 - Issue #165
June 22nd, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Building Secure Email Accounts & Profiles

People take email for granted, you get your email, read it, answer it, and move on. But how do you know who else is trying to access your account? Here are a few suggestions for securing your email:

1. Once again, make sure you are using a long, strong and unique password that isn't used anywhere else.
2. Enable two-step verification. (Explained Below.)

3. Look at your account history and sent items folder to see if anyone, other than you, has accessed your account recently.
4. Backup and delete any old email that you no longer need, especially email that might contain sensitive data like old passwords or financial information.
5. Don't check your email on public WiFi networks. (Unless you have a VPN activated.)
6. For the ultimate protection, consider using a "Whitelisting" program with your email.

Whitelisting your email account is specifically allowing emails from a certain source, such as any email from House of File Technologies, or certain friends and family members, to be allowed into your email inbox. By doing this all other email will be stopped by your junk or spam filter and will not be able to infect your device with anything malicious. Creating a Whitelist is a great solution for getting your email account usable again by stopping all of the spam. Adding such trusted email addresses to your whitelist so that they can pass easily through your spam filter or junk folder varies across the different email clients and internet security platforms.

Basically, you enable Whitelist functioning by adding trusted email addresses, friends or clients emails, or other emails you want to receive to your address book or contact list, then set your spam/junk filters to block all email not on this list. (Note you should check your spam email periodically to make sure it is not blocking emails you do want to receive. If so, add that email to your list for delivery.)

A whitelist is also helpful when you sign up to receive information or newsletters from a website. The email address that the newsletter comes from can be manually added to the whitelist so that the recipient can receive it, and it isn't filtered as spam. A newsletter doesn't have a way to verify its identity through a challenge response system; so unless the user puts the email address on the whitelist, the sender of the newsletter will be filtered as spam.

If you don't already have two-step authentication enabled on your email accounts, you really *need* to turn it on for anything sensitive. Two-step, or two-factor, authentication protects your accounts by requiring you to provide an additional piece of information after you give your password to get into your account. In the most common implementation, after correctly entering your password, an online service will send you a text message with a unique string of numbers that you'll need to punch in to get access to your account.

The idea is that you're drastically more secure if somebody needs both your password and the physical phone to get access to your accounts. Add a passcode to your phone, and you're safeguarded against someone stealing both. Is it perfect? No. But it's way better than just irrationally hoping nobody ever gets a hold of your password.

Two Step Verification is offered by Apple, Microsoft & Google and adds an very important level of security to your accounts. While your password is used to verify you, the 2nd step in using Two Step Verification requires that you verify your device. This is done by texting you a PIN Number whenever there is an attempt to access one of your accounts from a different computer/device than is registered to you. Thus, if someone does have your Email or Cloud password, they still could not hack your account without having your mobile phone to receive the PIN Number.

If you are creating a profile your email account, or for any social site, think of your profile as your "secret identity". You do not want to provide any information that would compromise you in your real life. (Unfortunately, this is not ethical on legitimate dating sites, but you should make sure that important personal information is only available upon request.)

Here are a few things to think of as you develop this secret identity:

1. Use a cartoon or avatar of yourself for your profile rather than a real image or picture.

2. Use a nickname rather than your real name. (Even stay away from initials.)
3. Don't enter any personal things about yourself that would be recognized by anyone that knows you.
4. Don't reveal your address, real phone number, or place of work in your profile. (Not even your town, only refer to a region.)
5. Be very generic about your age, a few years one way or the other doesn't make a difference.
6. Make sure the security settings on your profile are set to private, and only shared to approved friends/followers. (This is sometimes tricky because there are sites that have the defaults concerning to profiles set to "public", and your privacy settings can mysteriously change back to the default setting with you realizing it happened.)

Thank you for subscribing to our email!