Email Security

Email Guides

GENERAL INFORMATION

While it's convenient to know that you can send information quickly through electronic mail, it's important to remember that the information you send and receive is not secure. The following are some tips to keep your private information private. If you have any additional questions or require further information, it is available in the ***IT Help Desk or by calling (410) 677-5454.***

DON'T OPEN UNEXPECTED ATTACHMENTS

Never open an attachment without first knowing what it is. Many viruses, key-loggers, and other security risks are sent through attachments. Verify with the sender that they have sent you an attachment and never open an attachment you have received unexpectedly. In addition, before opening your attachment, save the attachment to your desktop, right-click the file and choose Scan for Viruses to ensure that the file is free of viruses.

DON'T CLICK LINKS IN AN EMAIL MESSAGE

Often times "phishing" emails attempt to disguise illegitimate links as seemingly safe looking links in order to extract personal information. In addition, many key-loggers disguise themselves as links to items that don't seem harmful, such as picture files. Hovering your mouse over a link will often allow you to see the true destination of the link.

BE WARY OF "FROM" AND "REPLY TO" ADDRESSES

These can be easily forged. Try asking for additional confirmation when you are unsure.

NEVER GIVE OUT PERSONAL INFORMATION BEFORE VERIFYING WHO IS ASKING

It's a good idea never to give out such information through email, as many "phishing" emails attempt to gather personal information by posing as a legitimate company asking for those items. However, if you must send out that information, ask for verification from the sender or company first. Usually a visit to their website (typed in, not through a link in the email) or a phone call is enough confirmation.

BE CAREFUL SENDING SENSITIVE INFORMATION THROUGH EMAIL

Remember, email isn't like a sealed envelope. It's more like a postcard. Once it leaves your mailbox, you have no control over who reads it. It could be intercepted, could have been sent to the wrong address, or it could be forwarded to someone you didn't intend to have it. This is especially true concerning personal information, such as usernames, passwords, social security numbers, bank account information, phone numbers, addresses, etc. However, it is equally true of any sensitive document or information you may send, such as proprietary information, confidential correspondence, research, and the like. A good rule of thumb is not to send anything by email you wouldn't want to see on a billboard on your way home.

CHOOSING A GOOD PASSWORD

WHAT ARE GOOD PASSWORDS AND WHY DO I NEED THEM?

Today, computer crackers are extremely sophisticated. Instead of typing random password by hand, crackers use personal computers to make phone calls repeatedly to test passwords in an effort to penetrate security. Even a modest home computer with a good password-guessing program can try thousands of passwords in less than a day's time. Some hit lists used by crackers contain several hundred thousand words. Therefore, any password that someone else might guess is a bad choice.

WHAT IS MY PASSWORD REQUIRED TO BE?

Your password must be a minimum of fourteen characters long, and can be any combination of at least three types of the following: upper and lower case letters, numbers, and any of the symbols over the numbers on the keyboard except **^ [in other words, ~,!,@,#,$,%,&,*,(, and)].**

WHAT PASSWORDS SHOULD I AVOID?

- Avoid using your name, your spouse's name, your parents' names, or your pet's name as a password.
- Other bad passwords are these names spelled backwards or followed by a single digit.
- Also avoid things that are listed elsewhere, like your address, zip code, phone number, Social Security Number, Driver's License Number, License Plate number, etc. Remember all of these are likely accessible by the public and can therefore be used to crack passwords.
- Short passwords are also bad, because there are fewer of them and are more easily guessed.
- Especially bad are words from computer games.
- Other bad choices include phone numbers, characters from favorite movies or books, favorite drinks, or famous people.
- Words in any dictionary.
- Your user name.
- Anyone's name (crackers don't necessarily know that your aunt's middle name is Agnes, but it's easy enough to get a list of 100,000 names and try each one).
- Any word in any ``cracking dictionary.'' There are lists of words that crackers use to try to crack passwords: passwords that a lot of people use. Some of these lists include:

  Abbreviations, Asteroids, Biology, Cartoons, Character Patterns, Machine names, famous names, female names, Bible, male names, Movies, Myths-legends, Number Patterns, Short Phrases, Places, Science Fiction, Shakespeare, Songs, Sports, Surnames

- Any of the above, with a single character before or after it (``8dinner'', ``happy1'').
- Any of the above, capitalized (``cat'' --> ``Cat'')
- Any of the above, reversed (``cat'' --> ``tac''), doubled (``cat'' --> ``catcat'') or mirrored (``cat'' --> ``cattac'').
- We used to tell people that taking a word and substituting some characters (a 0 (zero) for an o, or a 1 for an l) made a good password. This is no longer the case. New crackers have the capability to crack things like this, in certain situations.
- Words like ``foobar'', ``xyzzy'' and ``qwerty'' are still just plain words. They are also popular passwords, and the crack programs look for them. Avoid them.
- Any of the sample passwords, good or bad, mentioned in this document.

HELPFUL TIPS FOR CHOOSING A GOOD PASSWORD

- Include digits and punctuation characters, as well as letters.
- Choose something easily remembered so it doesn't have to be written down.
- Use at least 14 characters. Password security is improved by having long passwords.
- Use two short words and combine them with a special character or a number, like ROBOT4ME or 2MATO4YOU.
- Put together an acronym that has special meaning to you, like NOTFSWFM (None Of This Fancy Stuff Works For Me) or ALPEGCAN (All Law Professors Eat Green Cheese At Night).
- In general, a good password will have a mix of lower- and upper-case characters, numbers, and punctuation marks, and should be at least 6 characters long. Unfortunately, passwords like this are often hard to remember and result in people writing them down. Do not write your passwords down!
- The license plate rule: take a phrase and try to squeeze it into fourteen characters, as if you wanted to put it on a vanity license plate.
- Some people like to pick several small words, separated by punctuation marks of some kind.
- Put a punctuation mark in the middle of a word, e.g., ``vege%tarian''.

- Use some unusual way of contracting a word. You don't have to use an apostrophe.
- Avoid control characters. A lot of them have special meanings. If you use ^D, ^H or ^U, for example, you might not be able to log in again.
- Think of an uncommon phrase, and take the first, second or last letter of each word. ``You can't always get what you want'' would yield ``ycagwyw''. Throw in a capital letter and a punctuation mark or a number or two, and you can end up with ``yCag5wyw''.
- Deliberately misspelling one or more words can make your password harder to crack.
- Use several of the techniques above.
- Something that no one but you would ever think of. The best password is one that is totally random to anyone else except you. It is difficult to tell you how to come up with these, but people are able to do it. Use your imagination!

Tips on safeguarding your password

- First and foremost, NEVER give your password to anyone. ``Anyone'' means your coworkers, your spouse, your systems administrator. In the event of an emergency, the IT Help Desk can change your password. Your systems administrator or IT Help Desk never has a need to know your personal password. If someone needs to get onto our machines, and has a reason to be here, do not give them access to your account. Speak to the IT Help Desk staff about us setting up an account for them. We would be very happy to give them one.
- Make your password something you can remember. Do not write it down. If you really, honestly forget your password, we can easily give you a new, temporary one. We'd rather set your password once a month because you forgot it than have someone find it written down and gain unauthorized access to your account.
- Make your password difficult for others to guess. This is not as hard as it initially seems. See the section above on choosing a good password.
- DO NOT change your password because of mail from someone claiming to be your systems administrator, supposedly needing access to your files!! This is a popular scam in some circles. Remember, your systems administrator never needs your password for any reason. If someone needs to ask you to change your password so that they can gain entry to your account, they do not have reason to be there.