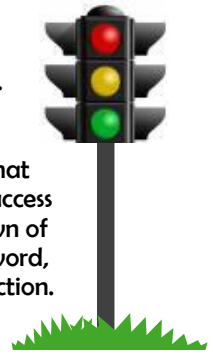


Know Passwords – No Compromise

Over the past several weeks CAS has noticed an increase in compromised Extension email passwords.

A compromised password is a password that has been phished or captured and is now being used without the knowledge or permission of the email account's owner (that's you). Why are compromised passwords important? If your email password has been compromised that means that someone can use your email account to send SPAM mail (Viagra, porn, lottery, etc) in your name, access bank accounts and lots of other things that are sure to ruin your day! Take a look at the breakdown of green light, yellow light, and red light passwords listed below. Green means you have a great password, yellow means you're treading on dangerous ground, and red means you need to take immediate action.



A **GREEN** Light Password:



- ✓ Is a password that is between 6-8 characters long (letters and numbers)
- ✓ Does not contain your username in it (ex. If your username is adamb your password should *not* be adamb1)
- ✓ Your password is made up of letters that represent an acronym or phrase (ex. If you use the phrase: "Safety rules are your best tools" and let's say you started working for Extension in 2008 your password could be: 2SRAYBT8)
- ✓ Has not been shared with anyone else
- ✓ Is an Extension email password that has NEVER been entered as a password anywhere else (ex. You've never used your Extension email password for a MySpace account, a bank account, etc.)

A **YELLOW** Light Password:



- ✓ Is a password that might have been shared with another person in the office but they would "never do anything bad with it"
- ✓ You can't really remember if you've responded to a phishing email or not –maybe you did, maybe you didn't
- ✓ You might have used the same Extension email password for your Wal-Mart Photo password but c'mon, you can trust Wal-Mart, right?
- ✓ You checked your Extension email at the local library and the computer asked if you wanted it to remember your password

A **RED** Light Password:



- ✓ Is a password that has been shared with others in the office
- ✓ Is a password that has been used for bank accounts, or "fun" websites (MySpace, Google Earth, Yahoo!, etc.)
- ✓ Has been used at public computers (like in a hotel lobby or airport kiosk), this type of computer could have capturing software that "captures" your password
- ✓ Is a password that is being used with an email account to SPAM other users' Inbox.

So what light did you get stopped at? If you stopped on green, congratulations – you're good to go! If you got stopped on a yellow or red-light it's time to reset your password. How do you reset your password? Simple, just fill out the attached Reset Password form and fax it to Computer Applications and Services at 1.662.325.8761, attention Password Reset. You should expect the password reset to take 1 full business day. If you cannot login to email with your old password try the new password. Remember your email password also controls your access to the X drive as well as your initial Intranet login.

Please Note: No passwords will be accepted or given out over the telephone.