The Best Email Security Is a Strong Password That Is Unique Only to You

Weak passwords won't protect your work at ACES or your personal information from data theft or hacking. Think about the passwords and phrases that people use in your office or building daily. Stray from common terms and language. Be creative! Read below to strengthen your defense against internet vulnerabilities based on the tips we share.

A strong and secure password is almost impossible to guess without some insight. Hackers may attempt to break into your system using specialized password-guessing software, but you can make it impossible even against software that can work through millions of combinations to breach your email account.

Sometimes, the hacker may not even require software if they can reference your information online. The more complex the password, the more time it takes for the software to solve the code. The passwords that follow our best practices outlined below would still take 100 years to crack.

Essentials for a strong password:

- **Optimally aim for 12 characters, minimum:** You need to choose a password that's long enough to set yourself up for success and safety. There's no minimum password length everyone agrees on, but you should generally go for passwords that are a minimum of 12 to 14 characters in length. A longer password would be even better.
- **Include numbers, symbols, capital and lower-case letters:** Use a mix of different types of characters to make the password harder to crack.
- **Never use your birthday, family name, hometown, address, school, university, or brand.**
- **Avoid common letter-number substitutions:** Don't Rely on Obvious Solutions or Substitutions: Don't use common substitutions, either — for example, "H0use" isn't strong just because you've replaced an o with a 0. This is an obvious solution for a well-experienced hacker.
- **Think in terms of phrases rather than words**
- **Don't use common dictionary words:** Stay away from obvious words and combinations of dictionary words. Any word on its own is not advisable. For example, "house" is obvious. "Red house" is even more obvious, especially if you reside in a red house!

Protecting Ourselves Against the Most Common Type of Cyber Attack

Note: If you encounter this, we recommend priority attention with a voice call from you for rapid response by the ACES Cyber Breach Team (Ext. 13310). Phishing attacks are the act of sending fraudulent communications that are sent from a seemingly reputable source. Phishing is an online con game, and phishers are nothing more than tech-savvy identity thieves. They use email messages, malicious websites, and instant messaging to trick people into disclosing personal information. It is usually done through email. However, the reputable source is not as it seems. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine. Malware is software that is designed to disrupt, destroy, or allow a hacker to gain unauthorized access to a computer's operating system. Phishing attempts can span many techniques from fake emails and pop-up ads to even phone calls.

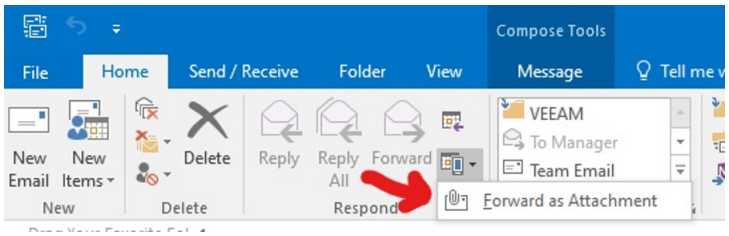
Essentials for your protection:

How to help protect yourself against email phishing scams:

- If you recognize an email as suspicious, do not click on any links contained or download any attachments. Instead, open up your web browser and go to the website in question by typing it into the URL bar.
- Be cautious and pay attention! Phishers have been known to use real company logos to make their communications seem legitimate. They will use email addresses similar to an actual company address. However, the address may be misspelled slightly or come from a different domain.
- Never give anyone personal information over the phone. Hang up, locate the phone number of the company on their website. Contact them all directly to determine the legitimacy of the call or the company.
- Never call the number the caller provides. When looking up the company website, make sure it is legitimate.
- Never allow anyone remote access to your computer.
- Examine a suspicious email message closely. Look for obvious signs of fraud such as poor grammar or misspelled words and unprofessional imagery
- When in doubt (never click on a pop-up), open up your antivirus software and run a system scan right away.
- Customer support from a security software such as Norton or McAfee will never send users unsolicited pop-ups stating that they will fix a user's computer if given remote access. Be watchful. **When a staff member at ACES requires support, the ACES Tech department can remote into an ACES machine using Splashtop, (sos.splashtop.com) as our remote access tool.**
- If you come across a suspicious website, examine the URL closely. Often times, cyber villains will create fake websites by registering a domain name that looks similar to the URL of the legitimate site they're duplicating.
- Use a secure search service to ensure the site you are about to visit is safe.

If You Have Been the Victim of a Scam

- Stay Calm.
- Be Efficient.
- Take notes on the process you are about to begin.
- Notify acesbreachnotice@aces.org. Forward the e-mail as an attachment. The ACES Cyber Team will receive the header of the e-mail and can analyze it safely. In this format we can send it to MS-ISAC Center for Internet Security if it is deemed necessary.



If You Have Been the Victim of a Scam (continued)

- Run a Full System Scan for viruses on your computer.
- Change your passwords right away.
  - Your computer
  - Online banking or financial institutions
    - Contact your bank to report fraud if your account has been compromised
  - Your personal email accounts
  - Any other password-protected websites that you visit regularly

Watch for our next newsletter in November

- Recommended Software Security
- Password Sharing
- Whaling versus Pharming
- Teaching Students to Be Critical & Watchful Users
- The SeeSay Initiative