Computer Crime Investigative Unit
U.S. Army Criminal Investigation Command

Cybercrime Prevention Flyer

CPF 0001-17-CID361-9H

06 February 2017

Protect Your Personal Email Account

The World is Connected by Email

If you are on the internet, you use email. Worldwide, more than 200 billion emails are sent every day. For many, email is their primary method of communicating with others in the wired world—often preferring email to other forms of communication because it is "more efficient." Email is used so frequently and for such a broad range of things, people's lives are pretty well chronicled in their emails.

Results of a recent Adobe email survey show email is a widely accepted part of our daily lives.

- About half of email users expect a response to their sent email within an hour.
- More than three-fourths of email users check work email while on vacation and nine out of ten workers check personal email while at work.
- Checking email during conversations is now acceptable.

Email can be risky and you could be vulnerable. Care should be taken to secure your email. The website, IdentityForce, reports that in 2016 more than 2 billion email addresses and passwords were compromised in some manner. If you have work email, follow your employer's guidelines. In the absence of work guidelines and for your personal email, consider these important email safety tips.

Tips for Email Safety

Passwords

Passwords, secret elements of authentication, are on the front line of defense preventing people and automated tools (e.g., password crackers) from illegally accessing your online accounts. Therefore, your choice of password and the frequency with which you change it are important security considerations.

A password, however, need not be limited to a single word. It can be a passphrase. A passphrase is a string of characters that form a phrase. An example might be, "The song remains the same" or "I'll see you on the dark side of the moon". Passphrases are generally easier to remember than complex passwords and are more likely to survive a dictionary attack than is a single word.

Handle your passwords as you would any personal and confidential information. Do not share any of them with anyone. Anyone asking you to divulge your password is undoubtedly a scammer. Be wary of emails you receive asking you to click a link and resubmit account particulars. That email might very well be a phishing attempt.

Contact Information:
Cyber Criminal Intelligence Program
27130 Telegraph Road
Quantico, Virginia 22134

Phone: 571.305.4482 [DSN 240]
Fax: 571.305.4189 [DSN 240]

Email

CCIU Website

CID Cyber Lookout
On Point for the Army

DISTRIBUTION:
This document is authorized for the widest release without restriction.

"DO WHAT HAS TO BE DONE"

Guidelines for passwords to **avoid** include:

- Your name or any permutation of your name
- Your user ID or any part of your user ID
- Common names
- The name of any relative, child, or pet
- Your telephone number, social security number, date of birth, or any combinations or permutations of those
- Vehicle license plate numbers, makes, or models
- The school you attended
- Work affiliation
- The word "password" or permutations including "password" prefixed or suffixed with numbers or symbols
- Common words from dictionaries, including foreign languages
- Names or types of favorite objects
- All the same digits or all the same letters or letter sequences found on keyboards

Password Recovery Questions

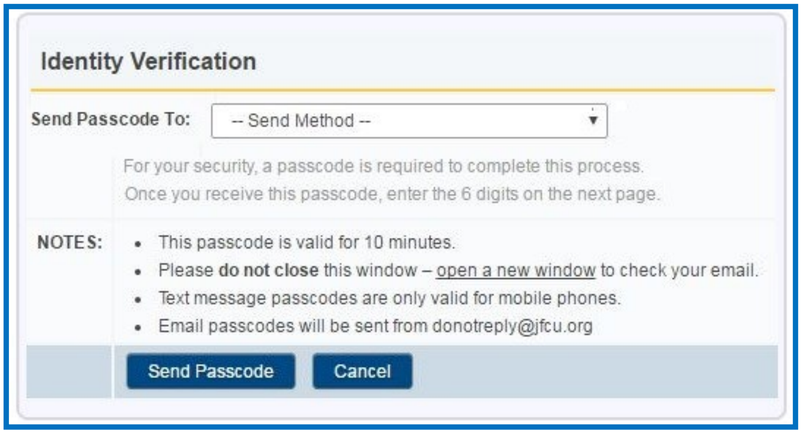
Forgetting passwords, especially if you opt for a complex password rather than a passphrase, is easy to do. Many sites use password recovery or security questions as a backup method to identify you if you forget your password. If you have the option of picking security questions, use those that the answer to cannot be easily guessed.

Two Factor Authentication

Although nothing is guaranteed to protect you in all situations, two factor authentication is the best way to prevent someone from accessing your accounts. If your email provider allows two factor authentication, use it.

With two factor authentication enabled, any attempt to access your email account triggers an additional layer of protection. Access to your account will be interrupted and your provider will send a message with a temporary security code to your mobile phone. To complete the login process, you must successfully enter that security code.

With two factor authentication, a hacker trying to compromise your email account would need to have your email username, password and mobile phone to be successful! The two factor security code changes with each use and a specific code expires after a certain amount of time passes. Therefore, in order to compromise two factor authentication, a hacker would need to guess the same security code randomly selected by the email provider. The probability of guessing a six digit security code is a one in a million proposition.



Identity Verification

Send Passcode To: -- Send Method --

For your security, a passcode is required to complete this process.
Once you receive this passcode, enter the 6 digits on the next page.

NOTES:

- This passcode is valid for 10 minutes.
- Please **do not close** this window – open a new window to check your email.
- Text message passcodes are only valid for mobile phones.
- Email passcodes will be sent from donotreply@jfcu.org

Two factor authentication is known by many different names. Here, it is known as Identity Verification.

Use Multiple Email Addresses

Use a different email address for different facets of your life. For instance, one for financial dealings, one for online purchases and one for social emails. Also, using multiple email addresses for different facets of your life makes it easier to assess what information might have been compromised should a compromise ever happen.

Be Mindful of How You Access Your Email

Using publicly available computers at your local library, your hotel's business center or an internet café are quick and convenient ways to check email. But, without proper precautions, doing so could be unsafe.

If the computers are not properly configured or if anti-virus software is not being used, a hacker could install key logging software. Every keystroke, including your usernames and passwords for every site you log in to are saved and made available to the hacker. (The danger of this can be reduced with two factor authentication. See p. 2.)

After checking your email, log out of the account. Forgetting to do so could be devastating. The next person to use that computer could have complete access to your account. That would include access to your inbox, stored emails, deleted emails, attachments to any of your emails, and email settings. A fun-loving prankster could send embarrassing emails, nasty emails or threatening emails. And, those emails would appear to have come from you. With access to account settings, someone could change your password, effectively locking you out of your email—forever, or simply delete your account.

Equally important, after you have successfully logged out, close the browser you are using. An even better idea is to restart (reboot) the entire computer if it is configured to allow users to do so.

Always, when using a public computer, make certain that the option to "remember me" is never checked and, if prompted to save your password, do not.

Use and Update Anti-Virus Software

Up-to-date anti-virus software will detect programs on your computer that a hacker could use to compromise your online activity. These programs are often installed after viewing phishing emails or clicking links in emails and can record your keystrokes and allow hackers backdoor access to your computer.

Anti-virus software for personal use is available free of charge to military personnel and DoD employees at DISA Home Use Anti-Virus.

Additional Resources

How to protect your email account from hackers—National Fraud & Cyber Crime Reporting Centre, UK
Cybersecurity Practices Initiative—Texas Tech University
How to protect your email account from hackers—wikiHow
5 ways to protect your email account from hackers—The Evening Standard, UK
What to do when your email gets hacked—Techlicious.com

Disclaimer: The appearance of hyperlinks in this Cybercrime Prevention Flier (CPF), along with the views and opinions of authors, products or services contained therein do not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations.

ICE

CCIU uses the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide feedback.