# INFORMATION SECURITY TEAM MESSAGE:

# Four Steps to Staying Safe Online

**We can all help build a safer, more trusted digital world. Follow these four simple steps to stay safer online at home, work, and school. Share these tips with colleagues, family, and friends to help build a significantly safer online world.**

### 1. Use Strong Passwords

Strong passwords are long, random, unique, and include all four character types (uppercase, lowercase, numbers and symbols). Password managers like 1Password and LastPass are a powerful tool to help easily create strong passwords for every account. And when you use a password manager, you never have to search through scraps of paper or notebooks to find a password. Most include both desktop and mobile options, so your passwords are always at your fingertips.

### 2. Turn On Multifactor Authentication, aka, MFA

There's more you can and should do for security than just creating strong passwords for your online accounts. Enabling multifactor authentication (MFA) makes you significantly less likely to get hacked. MFA requires an extra step to log in, like entering a code that is texted or emailed to you, or using a related authentication app. The extra security is well worth the modest extra effort. Enable MFA on all your online accounts that offer it, especially email, social media, and financial accounts.

### 3. Recognize & Report Phishing

Be cautious of unsolicited messages asking for personal information. Be highly cautious about sharing sensitive information or credentials with any website, and never share with unknown sources. Banks and other financial institutions will never ask you to provide passwords, account numbers, or any other sensitive information in response to an email. At work, report phishing emails to your corporate help desk. At home, delete the phishing messages.

### 4. Update Software

Software is continuously updated as new threats or vulnerabilities are identified. Ensuring your software is up-to-date on all your desktop, mobile, and connected devices is the best way to make sure you have the latest security patches and updates. Enable auto-update or regularly check for updates if automatic updates are not available.

## USFHP at PacMed Information Security Team

**Don Carter**
Information Security Manager

**McCall Paxton**
Senior Information Security Engineer

**Abolaji Filani**
Information Security Analyst