Berkeley UNIVERSITY OF CALIFORNIA

Information Security Office

Information Technology

CYBERSECURITY IN A NUTSHELL

- Practice good password management
- Use 2-Step authentication to protect your CalNet account
- Install antivirus/anti-malware protection
- Avoid phishing scams
- Report cybersecurity incidents

CONTENTS

CYBERSECURITY IMPORTANCE

Our reliance on technology means that we are living in an increasingly complex and digital world. We can't control how our information is protected once it's exposed, but we do have some control over the information we choose to share in the first place. It's our responsibility to protect our information and the electronic resources of UC Berkeley.

In this booklet, you will learn:

- How to **secure** your CalNet account and devices
- How to **recognize** and avoid phishing scams
- How to **report** cybersecurity incidents

For more information, go to [security.berkeley.edu/education-awareness.](security.berkeley.edu/education-awareness)

SECURE YOUR CALNET ACCOUNT

THE IMPORTANCE OF CALNET CREDENTIALS

Your CalNet credentials allow you to log in to a wide range of services such as bMail, CalTime, Financial Aid, bCourses and transcripts. These services contain confidential information, including your financial records, employment details, health records and more. Developing safe habits helps prevent misuse of credentials and protects UC Berkeley's credibility as well as your own personal reputation online.

CALNET 2-STEP VERIFICATION

USING 2-FACTOR AUTHENTICATION

Using a 2-Factor verification service such as Duo ensures you are the only person able to access your account, even if your password is stolen. All employees, affiliates, and students are required to use 2-Step to secure their CalNet accounts.

TIPS AND BEST PRACTICES:

Enroll more than one device

To avoid getting locked out of your CalNet account, enroll more than one device to your 2-Step account and print your bypass codes. Remember that when you get a new phone or if your phone dies, you still need to use 2-Step to access all campus services. Don't get locked out on finals week! Be prepared.

Do the push!

Setting up the Duo Mobile app on your smartphone to send a Push notification is the easiest way to do a 2-Step.

Trust your browser

Select "Yes, Trust Browser" on a computer you regularly use and that you trust. This will allow your browser to remember your 2-Step login for 30 days. Do not select "Yes, Trust Browser" on a public or shared computer!

Use duo for other accounts

You can use Duo to add the security of 2-Factor authentication to other important accounts such as your Amazon, Coinbase, or bank accounts. For more information visit calnetweb.berkeley.edu/calnet-2-step/2-step-tips-and-best-practices.

PRACTICE GOOD PASSWORD MANAGEMENT

- Always use different passwords for each account, including your personal accounts.
- Never reuse your CalNet passphrase for other accounts.
- Use a Password Manager - UC Berkeley offers students a free LastPass Premium account (visit calnetweb.berkeley.edu/calnet me/lastpass-premium for more information).

Quick Links

calnetweb.berkeley.edu/calnet-me

security.berkeley.edu/education-awareness

security.berkeley.edu/resources

SECURE YOUR DEVICES & COMPUTERS

1. **Keep all softwares up to date**
   There are a lot of good reasons not to put off software updates. You get a better user experience, and more importantly, updates fix software bugs that can leave your systems and devices open to attack.

2. **Install antivirus software**
   Your computer will have built-in antivirus features that can help protect it from certain malicious code.

3. **Turn on your firewall**
   A firewall sits between a computer (or local network) and another network (such as the Internet), controlling the incoming and outgoing network traffic, adding another layer of protection.

4. **Use a password manager**
   Creating highly secure passwords for each of your personal and work accounts is easy with a password manager. Using strong and unique passwords on each of your accounts increases your personal and professional online security. UC Berkeley offers FREE LastPass Premium for all students, employees, and affiliates. For more information, visit calnetweb.berkeley.edu/calnet-me/lastpass-premium.

5. **Lock your devices**
   Set your devices to lock the screen after no more than 15 minutes of inactivity - shorter is better, especially for smartphones. This will prevent unauthorized users from accessing your data.

PROTECT YOUR SMART PHONES

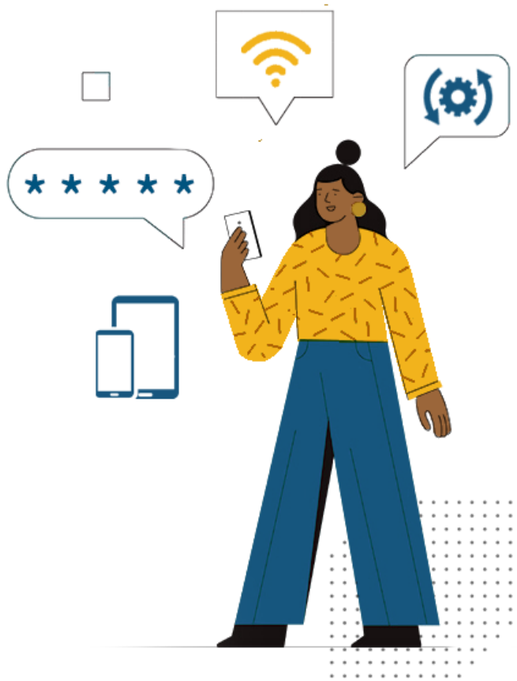
Use a password
Protect your devices with a complex password, PIN, pattern, or biometrics. If a device comes with a default password, change it right away.

Device updates
Regularly update your devices and apps. New updates often fix security vulnerabilities.

App management
Only download apps from reputable app stores like Google Play or Apple App Store. When downloading a new app, check the permissions you are granting. Unless the app requires your location, or requires access to your camera or microphone to work properly, do not allow it access or allow access only while using the app.

Open networks
Never allow your mobile devices to connect to a network without your permission.

Public Wi-Fi
Never share, enter, or access sensitive information when using public Wi-Fi. Others may be able to see your information when using unsecured Wi-Fi. Consider using a hotspot instead.



TECH SUPPORT FOR PERSONAL DEVICES

If you need help with your computer or suspect it may be infected with a virus, Student Tech Services (STS) can help! They provide free tech support to all undergraduate, graduate and professional students at UC Berkeley and can assist with:

- Resolving Wi-Fi problems and getting online.
- Installing and optimizing free campus software (including Adobe, Matlab, Microsoft, and Zoom).
- Troubleshooting device issues, e.g. blue screens, slow performance, data recovery, etc.
- Setting up CalNet 2-Step, obtaining a 2-Step hardware token and removing malware.
- Locating campus resources for printing, laptop lending, creative labs, and much more!

BACK UP IMPORTANT FILES

A backup is a second copy (or more) of your digital files, and it can protect you from losing your work if your device or data become inaccessible, destroyed, or damaged. Data loss can occur in many ways: a computer or hardware crash, a lost or stolen device, data corruption, or malware that encrypts your data and holds it for ransom.

TWO TYPES OF BACKUPS:

- Sync (or cloud) services back up individual files and do not include applications or programs. Google Drive and Box are examples of sync services and are available to all students for cloud backups. Learn more about these options at: technology.berkeley.edu/storage.

- Traditional backups enable a full system restore including programs, applications, settings, and files. Setting up an external hard drive with a backup program, like Time Machine, will back up your applications and data files and enable a full system restore. View all your options for backing up important files at security.berkeley.edu/backup.

PREVENT RANSOMWARE ATTACKS!

Ransomware is malicious software designed to block access to a computer system or data until a ransom is paid. Once a ransomware infection occurs, it may be too late to recover the encrypted information. Regular backups can help protect you.

HOW BACKUP SAVED THE DAY AT BERKELEY

Campus departments and individuals do experience ransomware attacks. In 2022, the Lawrence Hall of Science faced a ransomware attack via an email client. Additional attacks targeted the Centre of New Music and Audio Technologies and the Electrical Engineering and Computer Science division. In these cases, institutional data was saved by having backups!

LEARN TO AVOID PHISHING SCAMS

Phishing is a type of attack carried out in order to steal information or money from you. Phishing attacks can occur through email, phone calls, text or instant messages, and social media. Attackers are after things like your personal information: usernames, passwords, credit card information, and Social Security numbers. Phishing scams can have several goals, including:

Stealing from victims
Modifying direct deposit information, draining bank accounts.

Identity theft
Running up charges on credit cards, opening new accounts, and even impersonating you to scam friends and family.

Purchasing items
Buying gift cards, tricking victims into working on their behalf.

Getting access to the victim's computer
Clicking on malicious links can result in malware, spyware, or keylogging being installed on your devices.

Did you know?

UC Berkeley students have lost $30,000+ due to Fake job offers and bogus checks

Always contact professors through their contact information in the directory, and do not use a personal email account or a cell phone number that is not in the directory. This is the largest security concern impacting students as it deals with **financial loss**. Learn more at security.berkeley.edu/fight-phish.

HOW TO IDENTIFY PHISHING ATTEMPTS

The Information Security Office offers current examples of phishing emails and attacks reported on campus in the Phish Tank. These examples help show how to spot the phish. If you receive an email that seems suspicious, report it!
For more information, visit security.berkeley.edu/resources/phish-tank.

BROWSE SAFELY

Think about the websites you visit. Often, you will get asked to accept the site's privacy policies or terms and conditions. Some websites track other places you visit online and may collect personal data. Be familiar with privacy policies and terms and conditions.

REPORT CYBERSECURITY INCIDENTS

WHAT IS A CYBERSECURITY INCIDENT?

- Losing a university-owned device (including storage devices).
- Discovering malware on a device.
- Entering your CalNet credentials into a malicious website or through a phishing email.
- Falling for a phishing attack.

Even if you follow best practices and are extremely careful, you can still fall victim to a cybersecurity attack. If you receive notice that your account has been exposed or you want help securing your account, visit: security.berkeley.edu/respond.

Email:
security@berkeley.edu

Call:
(510) 664-9000
(option 4)

Important:
If an incident poses an immediate danger, contact UCPD immediately at
(510) 642-3333
or call 911

LET'S SEARCH FOR SECURITY!

V O S X K Q Z P H I S H I N G S C A M S
B A N O I O P A N T I M A L W A R E Y J
A M F O I J N C A R K X I P O C H G L X
C E L A K E A V L D D U U T H N R K E R
K Q O N S G C Y B E R S E C U R I T Y X
U U E A B O A A N D Z D N Q F A H K H U
P T W O S T E P M L E I L O R L G U T O
M U G Z W G Z U N J L A H C Z W J E Q M
M E I Q S H O O W F G H E D J Y W H R F
A I C P V A Z S T R U S T B R O W S E R
S T U D E N T T E C H S E R V I C E S O
N J U G A B L P D B X Z D G U K F W P P
H J C E F T B B Y O L J E Z C L M S H X
F O B H P Q C M A X T P B O E A W G I E
R X T X G H V F N R Z H Z G H S D K S P
G R A N S O M W A R E A E F M T E S H G
T W S A A B V R S C B Z D P Z P A U T M
L M Q A M E P W G P O T G Q U A M Q A X
F I R E W A L L N C F Y L M C S O Y N U
Q L X H I O W I N T E R C W D S H K K Z

Phishing Scams	Cybersecurity
Do the Push	Ransomware
Two Step	Antimalware
Trust Browser	LastPass
Phish Tank	Back Up
Student Tech Services	Firewall

Berkeley
UNIVERSITY OF CALIFORNIA

Information Security Office

Information Technology

Security is a shared responsibility...

For more information, go to security.berkeley.edu.

Email: security@berkeley.edu

Contact: (510) 642-3333 (emergency), (510) 664-9000