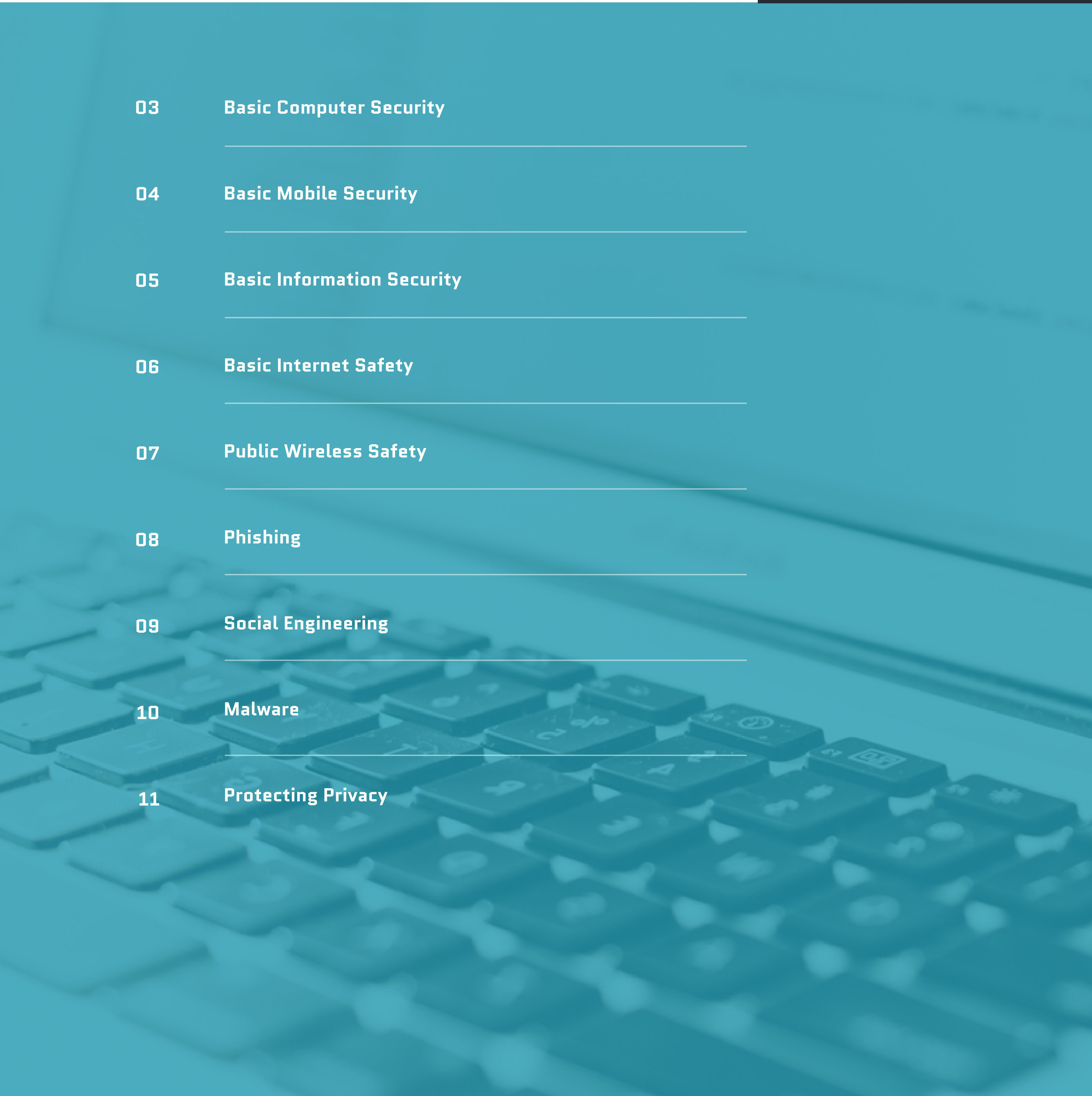
Coast Colleges

SECURITY AWARENESS

TABLE OF CONTENTS



BASIC COMPUTER SECURITY

Basic computer security starts with your own computer to help you build a foundation to further improve on. As technology changes you can adapt and improve upon the foundation.

Protection Tips

What you need to know

Help Desk Contact

(714) 438-8111 itservicedesk@cccd.edu

Current Operating System

The operating system is the most important software on your computer. It manages the hardware and software. Keep it updated with the latest security patches.

Update Software Applications

Software apps become outdated which creates vulnerabilities that can be exploited by cybercriminals. Keep all software apps updated to the latest version.

Use Strong Passwords

Weak passwords leave your computer and online accounts vulnerable to attack. Use strong and unique passwords for each account. Use a password manager like LastPass or KeePass.

Firewall On

Firewalls help protect your computer from unwanted connections. Keep your computers firewall turned on at all times.

Antivirus

Antivirus protects your computer from commonly known viruses. Use an updated antivirus software that detects modern threats.

Don't be Admin

An account having admin level rights can make any changes to the system good or bad. Don’t login to your computer using an admin account for daily activities.

Internet Browser Security

Keep browsers updated and don't ignore warnings. Verify plugins before you install. Don't save passwords and clear cookies.

Scan USB Devices

Scan USB storage devices before using them. Don't use shared USB devices.

Physical Security

Maintain physical control of your mobile devices and computers especially when traveling.

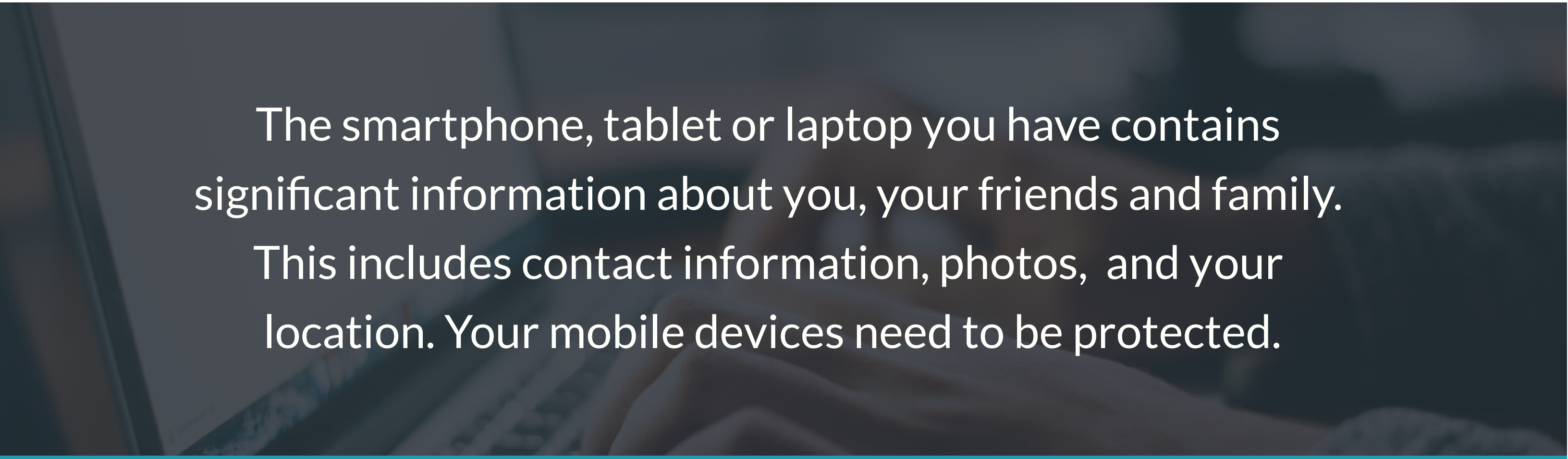
Check Apps Often

Check apps once a month to keep them updated and remove apps you no longer use.

Enable 2FA

Usernames and passwords by themselves are not enough to protect your accounts. Turn on two-factor authentication.

BASIC MOBILE SECURITY



The smartphone, tablet or laptop you have contains significant information about you, your friends and family. This includes contact information, photos, and your location. Your mobile devices need to be protected.

Protection Tips

What you need to know

Help Desk Contact

(714) 438-8111 itservicedesk@cccd.edu

Current Operating System

The operating system is the most important software on your mobile device. Keep it updated with the latest version and security updates.

Remove Unneeded Apps

Consider removing apps that are no longer used or needed.

Keep Apps Updated

Keep all your mobile apps updated. Consider setting updates to occur automatically.

Use Secure WiFi

Don't connect to open or unsecure WiFi hotspots.

Use a VPN

Consider using VPN software to keep your location anonymous and secure your information.

Enable 2FA

Usernames and passwords by themselves are not enough to protect your accounts. Turn on two-factor authentication.

Use Strong Passwords

Setup a passcode longer than 4 numbers. Use strong and unique passwords for each account and device. Use a password manager like LastPass or KeePass.

Suspicious Communication

Don't respond to fraudulent calls, texts, and voicemails.

Physical Security

Maintain physical control of your mobile devices and computers especially when traveling. Use only trusted charging stations.

Location Services

Location services are helpful when traveling, but they expose you location. Consider disabling when not in use.

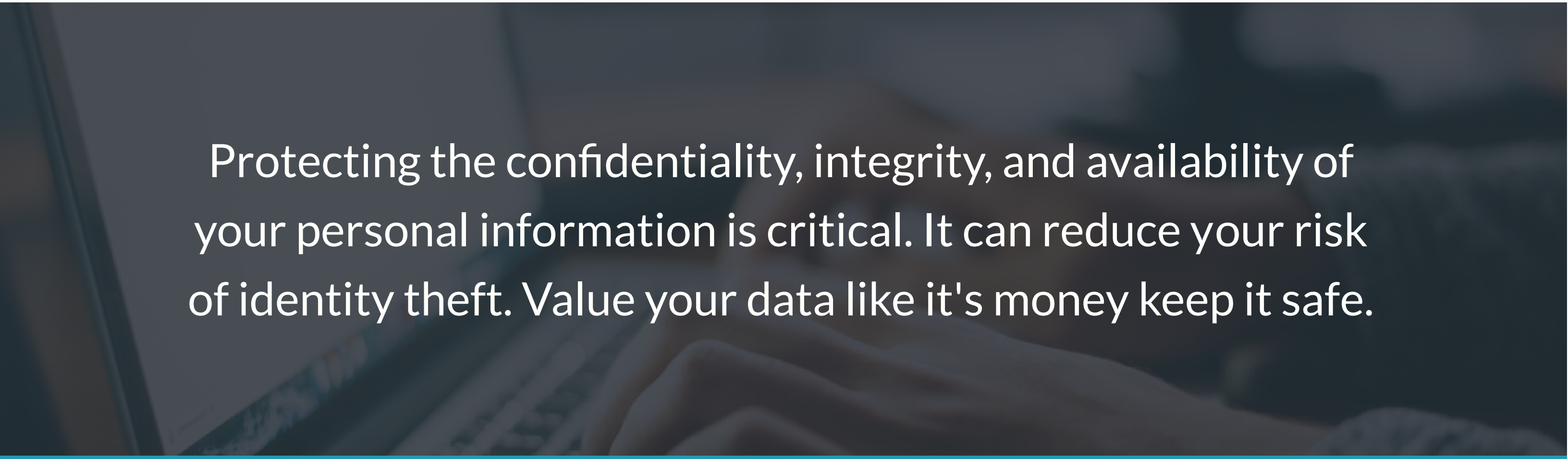
Find My Phone

Enable this feature so you can find, remotely wipe or disable your device if stolen or lost.

Back it Up

Backup your contacts, data and keep a copy off of the computer. Consider using cloud services for backups so you can restore to another devices or computer.

BASIC INFORMATION SECURITY



Protecting the confidentiality, integrity, and availability of your personal information is critical. It can reduce your risk of identity theft. Value your data like it's money keep it safe.

Protection Tips

What you need to know

Help Desk Contact

(714) 438-8111 itservicedesk@cccd.edu

Back it Up

Backup your data and keep a copy off of the computer. Consider using cloud storage for backups so you can access and restore to any device.

Turn on 2FA

Usernames and passwords by themselves are not enough to protect your accounts. Turn on two-factor authentication.

Share with Caution

Before you post online think about what others may learn about you. Never share personal financial information by email.

Keep Computer Clean

Use updated computer software and antivirus that detects modern threats and setup for automatic updates.

Use Data Vault

Consider using a password and data vault to store your personal information securely.

Physical Security

Maintain physical control of your mobile devices and computers especially when traveling.

Use Strong Passwords

Use strong and unique passwords for each account. Use a password manager like LastPass or KeePass.

Secure or Discard

Shred paper documents before you discard them. Use a utility program to securly erase data on computers.

Use Secure Sites

Use only secure sites that use HTTPS especially when providing your personal information.

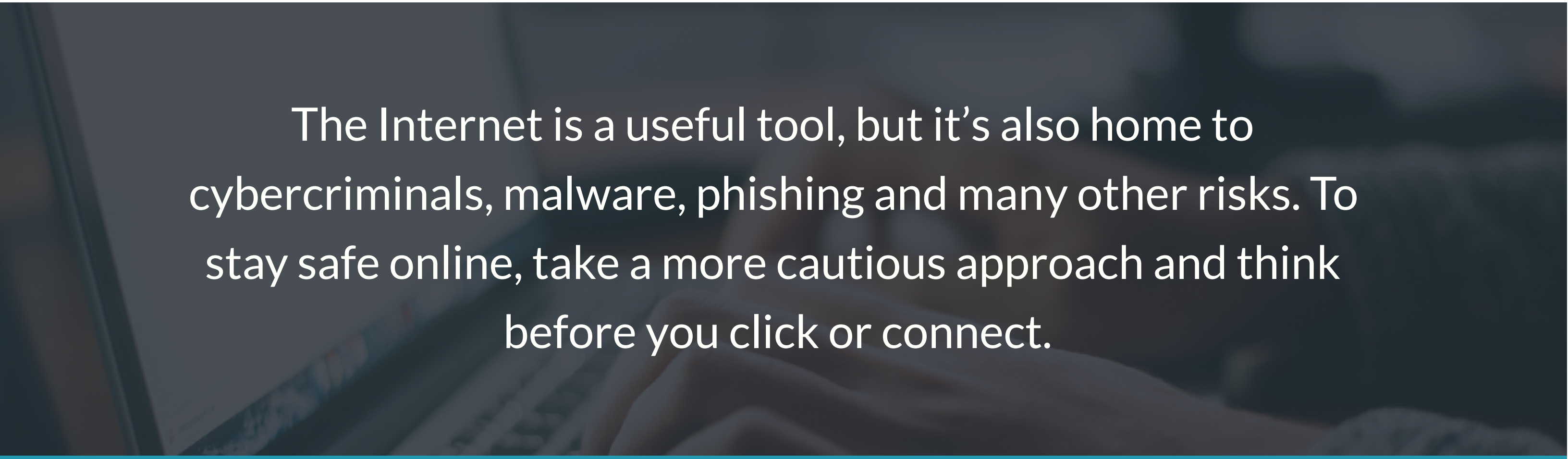
Keep Apps Updated

Keep all your software updated. Outdated apps can be affected by a vulnerability which exposes your information to attack.

Think Before Taking Action

Ignore emails, texts, or calls that create a sense of urgency, loss & demand you act immediately related to online accounts. Protect your information. If you are asked for your personal information, question why someone would need the information and whether you can trust them.

BASIC INTERNET SAFETY



The Internet is a useful tool, but it's also home to cybercriminals, malware, phishing and many other risks. To stay safe online, take a more cautious approach and think before you click or connect.

Protection Tips

What you need to know

Help Desk Contact

(714) 438-8111 itservicedesk@cccd.edu

Keep Computer Clean

Use updated computer software and antivirus that detects modern threats and setup for automatic updates.

Update Internet Software

Keep browsers and Internet software updated. Don't ignore warnings. Verify plugins before you install. Don't save passwords and clear cookies.

Use Trusted Search

Use trusted search engines, like Google, Bing and Yahoo. Think before you click on links, popups or ads.

Firewall On

Keep your computers firewall turned on at all times and your software updated.

Social Media

Don't stay logged in to social media accounts when browsing websites.

Keep Privacy Settings On

Both marketers and cybercriminals can learn a lot from your browsing and social media usage. Enable privacy settings.

Antivirus

Antivirus protects your computer from commonly known viruses. Use an updated antivirus software that detects modern threats.

Websites

Use caution when typing in website addresses. Be carful about what sites you visit. Don't click on ads or popups.

Downloads

Don't download files or software from untrusted websites. Office documents and PDFs can contain viruses. Use caution when downloading apps.

Use a VPN

Consider using VPN software to keep your location anonymous and secure your information.

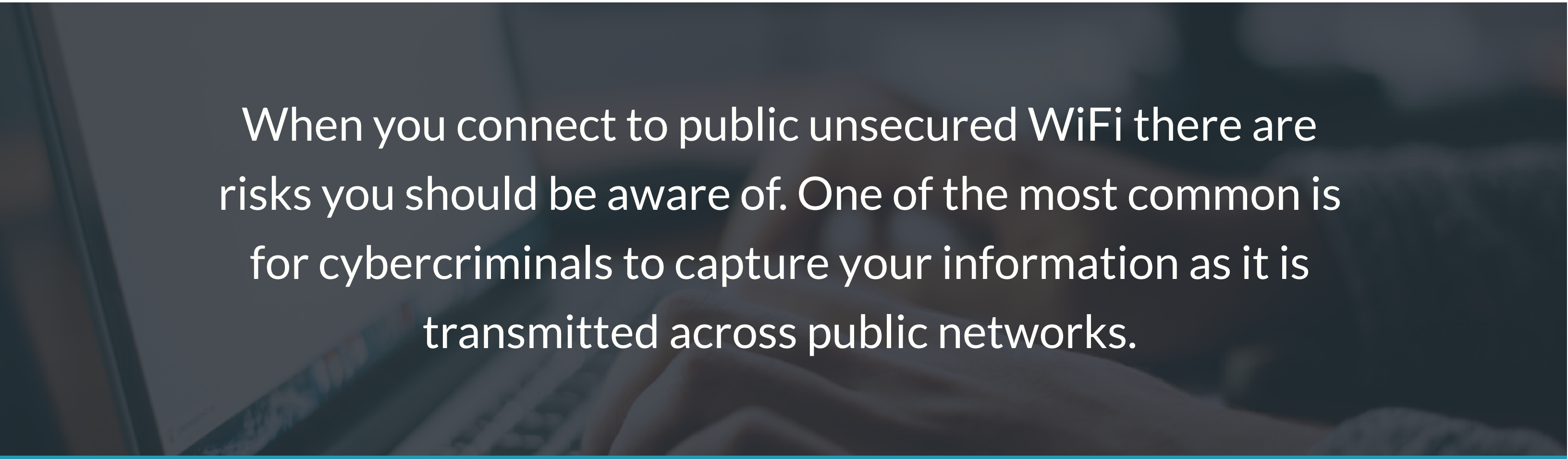
Use Secure WiFi

Don't connect to open or unsecure WiFi hotspots.

Security Through Education

Educate yourself about the types of threats to your privacy and security, it is one of the best defenses you have.

PUBLIC WIRELESS SAFETY



When you connect to public unsecured WiFi there are risks you should be aware of. One of the most common is for cybercriminals to capture your information as it is transmitted across public networks.

Protection Tips

What you need to know

Help Desk Contact

(714) 438-8111 itservicedesk@cccd.edu

Use Secure WiFi

Don’t connect to open or unsecure WiFi hotspots. Consider using your phone as a hotspot.

Use a VPN

Consider using VPN software to keep your location anonymous and secure your information.

Update Internet Software

Keep browsers and Internet software updated. Don't ignore warnings. Verify plugins before you install. Don't save passwords and clear cookies.

Firewall On

Keep your computers firewall turned on at all times and your software updated.

Turn on 2FA

Usernames and passwords by themselves are not enough to protect your accounts. Turn on two-factor authentication.

Financial Transactions

Don't connect and perform financial transactions over public WiFi networks.

Turn off Sharing

Turn off sharing of resources on your computer when using public WiFi.

Keep Computer Clean

Use updated computer software and antivirus that detects modern threats and setup for automatic updates.

Use Secure Sites

Only visit websites that use HTTPS or secure sites.

Verify WiFi Connections

Make sure you connect to a legitimate network. Verify the name and login information with the business. Don't automatically connect to WiFi networks.

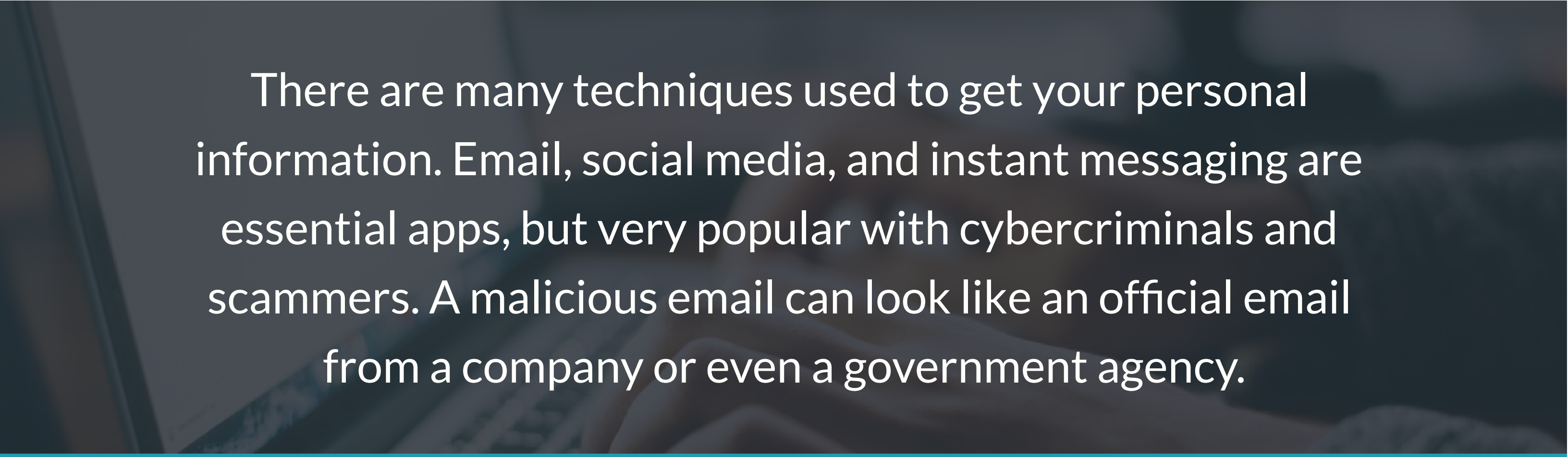
Disable File Sharing

Disable file sharing on your laptop or device if enabled.

Antivirus

Antivirus protects your computer from commonly known viruses. Use an updated antivirus software that detects modern threats.

PHISHING


There are many techniques used to get your personal information. Email, social media, and instant messaging are essential apps, but very popular with cybercriminals and scammers. A malicious email can look like an official email from a company or even a government agency.

Protection Tips

What you need to know

Help Desk Contact

(714) 438-8111 itservicedesk@cccd.edu
Report Phishing Emails: phishing@cccd.edu

Think Before Taking Action

Ignore emails, text messages, and phone calls that create a sense of urgency, loss and demand you act immediately related to online accounts or financial opportunities. Note: If you feel you were a victim of phishing, please contact the help desk via the above information.

Website Forgery

Cybercriminals build websites that mimic legitimate websites with the goal of deceiving you to provide sensitive information. If a site looks suspicious search for it online and contact them directly.

Suspicious Email

Delete suspicious email you didn't expect to receive. A hacked account from someone familiar can trick you. Ask yourself "Am I expecting this email?"

Email Links

Pay attention to links that appear legitimate. Use your mouse to hover over a link (don't click) to see if the company domain name is valid. Do your research to verify the organization.

Email Attachments

Don't open attachments you didn't expect to receive.

Email Services

Consider using email services that have built in anti spam and anti phishing technology.

Keep Devices Updated

Keep all devices and their software apps updated.

Email Phishing

Most phishing attacks are sent by email that appear to be from a legitimate organization. Used to steal sensitive information.

Vishing

A phone call where a scammer uses manipulation to get you to share personal information or account details.

SMiShing

Similar to Phishing however text messages are used to trick you into clicking on a link or sharing information.

Spear Phishing

Emails that target a specific person or department using phone calls, texts, or emails in order to steal your login or confidential information.

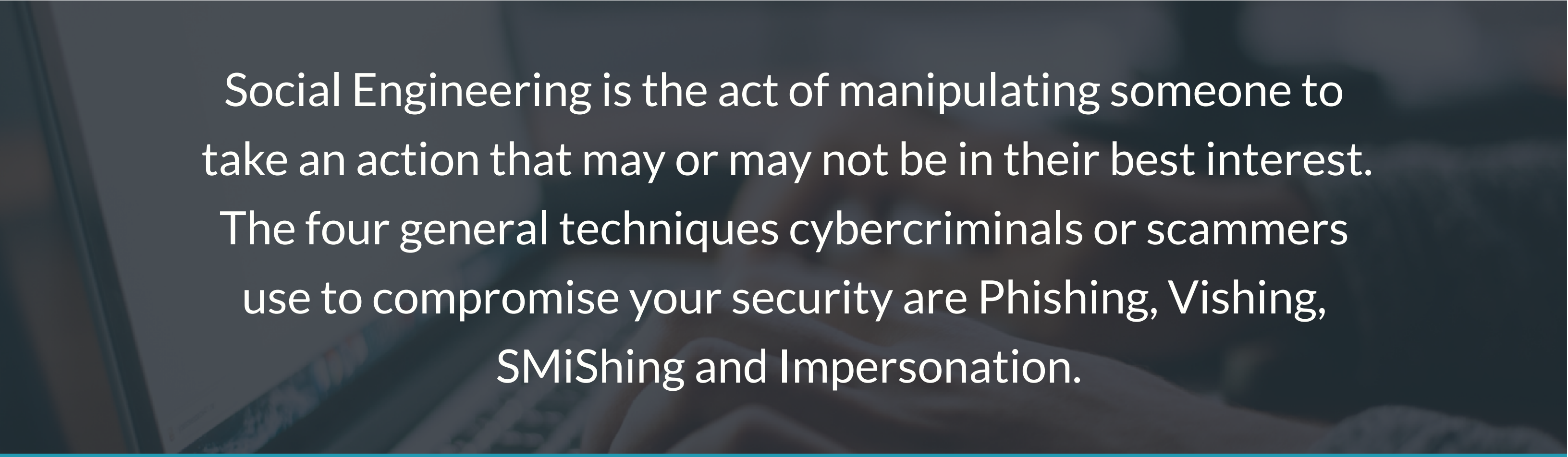
What to watch out for

- Suspicious sender's address
- A sense of urgency, fear or loss
- Too good to be true scams
- A generic greeting
- Poor spelling and grammar
- Suspicious attachments Word, Excel or PDF
- Fake emails that mimic a legitimate company
- Invoice attachments you don't expect to receive.

Why do we fall for it

- Greed
- Urgency
- Curiosity
- Fear
- Complacency
- Helpfulness

SOCIAL ENGINEERING



Social Engineering is the act of manipulating someone to take an action that may or may not be in their best interest. The four general techniques cybercriminals or scammers use to compromise your security are Phishing, Vishing, SMiShing and Impersonation.

Protection Tips

What you need to know

Help Desk Contact

(714) 438-8111 itservicedesk@cccd.edu

Phishing

Email and other types of messages that attempt to fraudulently get your personal information or install malware by masquerading as a trusted person or source.

Vishing

A phone call where a scammer uses social engineering to get you to share personal information or account details. Often voice recordings are used which transfer you to a live person.

SMiShing

Is similar to Phishing however they use text messages to trick you into clicking on a link to sharing person information or install malware on your mobile device.

Impersonation

When a person pretends to be another person for the purpose of fraud. This can be used by scammers and cybercriminals to impersonate a fellow employee or a person of authority to obtain personal information.

Education

Educate yourself about the types of social engineering attacks listed above.

Protect Your Devices

keep all your software and apps updated.

Use Caution

Be cautious of the information you give out. Don't give any personal or financial information over the phone or email.

What is known?

What do they know? Consider whether the person you are talking to has the need or right to the information they are asking for.

Research the Source

Check sources and call the official number when you are not sure a person is an official representative.

What is being asked?

Watch for questions that don't fit the persona or that pressure you to take action or make a decision immediately.

Real or too good to be true

Take the time to asses the situation and determine if it's realistic or not. Would the bank or company really contact you for account details? Be aware of get rich quick or financial scams.

Think before taking action

Ignore emails, text messages and phone calls that create a sense of urgency, loss and demand you act immediately related to online accounts or financial opportunities. Note: if you feel you were a victim of social engineering, please contact the help desk via the above information.

MALWARE

Malware is a general term that stands for Malicious Software which describes the specific types listed below. It is used to disrupt or damage a computer's operation or gain access to your computer and private information.

Protection Tips

What you need to know

Help Desk Contact

(714) 438-8111 itservicedesk@cccd.edu

Types of Malware

Viruses

A type of malicious app that is created to alter the computer and spread to other computer systems.

Rootkits

A Rootkit is malicious software that gives attackers full admin control of the computer.

Botnets

Use automated tasks to propagate malicious software that can connect back to servers on the Internet.

Key Loggers

Is a type of spyware that can monitor your activity and record your keystrokes. They can be used to steal passwords and banking info.

Trojan Horse

A Trojan Horse is a program that is disguised as legitimate software. Use caution, and only download from manufacturer website. Check customer reviews.

Spyware

Malicious software created to gather information & forward it to a 3rd party without your consent. It can be used to profit from your personal information.

Ransomeware

Malicious software that infects your computer and demands a ransom to unlock your data and fix your computer. Back up your data and keep it off the computer to protect yourself from this type of attack.

Worm

A computer worm is a malicious program that spreads over the network to infect other computers.

Use Modern Antivirus

Use updated antivirus software that detects modern threats like ransomware and set it up for automatic updates.

Back it Up

Backup your data and keep a copy off of the computer to protect it from malware. Consider using cloud storage for backups.

Firewall On

Keep your computers firewall turned on at all times and your computers operating system software updated.

Email Services

Consider using email services that have built in anti spam and anti phishing technology to help stop these emails from reaching your inbox.

Email Attachments

Think before you click links or open attachments Don’t open attachments you didn’t expect to receive. Delete the email.

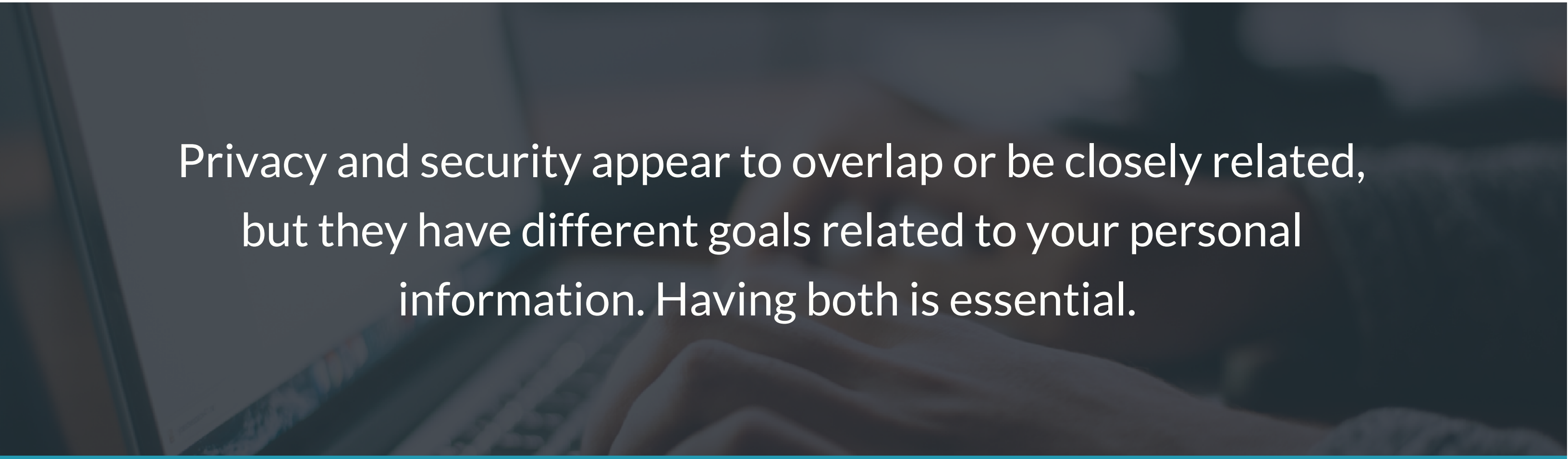
Scan USB Devices

Scan all USB storage devices before use. Don't use shared USB devices.

Keep Software Updated

Keep all software including your computers operating system, apps updated and patched to the latest versions. Check apps for updates regularly.

PROTECTING PRIVACY



Privacy and security appear to overlap or be closely related, but they have different goals related to your personal information. Having both is essential.

Protection Tips

What you need to know

Help Desk Contact

(714) 438-8111 itservicedesk@cccd.edu

Privacy vs Security

Privacy and security are considered to be closely related, but each of them have different goals. Privacy is related to your right to control your personally identifiable information (PII). Security is related to how your information is protected. You need to have both Privacy and Security.

What is PII?

Personally Identifiable Information also known as PII can include your name, address, date of birth, social security number and information related to medical status.

Data Breaches

A data breach occurs when someone gets unauthorized access to protected information. This can be your PII. The data is often shared without your permission.

Why it Matters?

The data stolen from breaches and other methods like phishing scams can be used to commit identity theft, compromise your accounts and cause financial loss.

Back it Up

Backup your data and keep a copy off of the computer. Make sure you have an accurate inventory of your PII, where its stored and who has access to it.

Physical Security

Maintain physical control of your mobile devices and computers especially when traveling.

Secure or Discard

Shred paper documents before you discard them. Use a utility program to securely erase data on computers. Reset and erase all portable devices before recycling them.

Use a VPN

Consider using VPN software to keep your location anonymous, secure your information and account access. Always use VPN software when connecting to open WiFi access.

Keep Track of Accounts

Keep an inventory of online accounts that have your personal identifiable information. Stay updated on which companies are affected by data breaches so you can take immediate action.

Limit Sharing on Social Media

Limit the amount of information you share on social media platforms.

Internet Browsing

Use your web browser in private mode when searching or browsing the Internet. Avoid risky sites

Turn on 2FA

Usernames and passwords by themselves are not enough to protect your accounts. Turn on two-factor authentication.