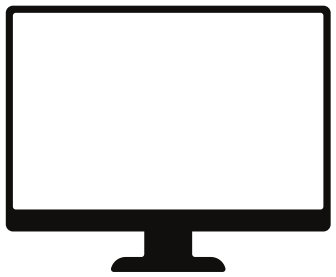
Computer Security

Scammers, hackers, and identity thieves are looking to steal your personal information – and your money. But there are steps you can take to protect yourself, like keeping your computer software up-todate and giving out your personal information only when you have a good reason.

- Use Security Software That Updates Automatically
- Treat Your Personal Information Like Cash
- Check Out Companies to Find Out Who You're Really Dealing With
- Give Personal Information Over Encrypted Websites Only
- Protect Your Passwords
- Back Up Your Files



Resources

Federal Trade Commission
877-FTC-HELP (382-4357)
http://www.consumer.ftc.gov
http://www.onguardonline.gov/

Department of Homeland Security
https://www.dhs.gov/topics/cybersecurity

SONOMA COUNTY SHERIFF'S OFFICE

Sheriff-Coroner Eddie Engram

707-565-2650

2796 Ventura Ave
Santa Rosa, CA 95403

sonomasheriff.org

Important Phone Numbers

Emergency……9-1-1
Dispatch (Non-Emergency).....565-2121
Business Line (Non-Emergency).....565-2650
River Sub-Station…….....……869-0202
Sonoma Valley Sub…….....……..…996-9495

SONOMA COUNTY SHERIFF'S OFFICE

Cyber Security

In partnership with our communities, we commit to provide professional, firm, fair, and compassionate public safety services with integrity and respect.

SONOMASHERIFF.ORG

Hacked Email or Social Media Account

You get a flood of messages from friends and family. They're getting emails from you with seemingly random links, or messages with urgent pleas to wire you money. It looks like your email or social media account might have been taken over. What do you do? For starters, make sure your security protections are up-to-date, reset your password, and warn your friends.

How You Know You've Been Hacked

- Friends and family are getting emails or messages you didn't send
- Your sent messages folder has messages you didn't send, or it has been emptied
- Your social media accounts have posts you didn't make
- You can't log into your email or social media account

What To Do When You've Been Hacked

1. Update your system and delete any malware

Make sure your security software is up-to-date. If you don't have security software, get it. But install security software only from reputable, well-known companies. Then, run it to scan your computer for viruses and spyware (aka malware). Delete any suspicious software and restart your computer.

2. Change your passwords

That's IF you're able to log into your email or social networking account. Someone may have gotten your old password and changed it.

3. Check the advice your email provider or social networking site has about restoring your account

You can find helpful advice specific to the service. If your account has been taken over, you might need to fill out forms to prove it's really you trying to get back into your account.

4. Check your account settings

Once you're back in your account, make sure your signature and "away" message don't contain unfamiliar links, and that messages aren't being forwarded to someone else's address. On your social networking service, look for changes to the account since you last logged in — say, a new "friend."

5. Tell your friends

A quick email letting your friends know they might have gotten a malicious link or a fake plea for help. Put your friends' email addresses in the Bcc line to keep them confidential.

What To Do Before You're Hacked

1**. Use unique passwords for important sites, like your bank and email**

That way, someone who knows one of your passwords won't suddenly have access to all your important accounts.

2. Safeguard your usernames and passwords

Think twice when you're asked to enter credentials like usernames and passwords. Never provide them in response to an email.

3. Don't click on links or open attachments in emails unless you know who sent them and what they are

That link or attachment could install malware on your computer.

4. Don't treat public computers like your personal computer

If it's not your computer, don't let a web browser remember your passwords, and make sure to log out of any accounts when you're done. In fact, if you can help it, don't access personal accounts — like email, or especially bank accounts — on public computers at all. (Also be careful any time you use public Wi-Fi.)

Disposing of Old Computers or Mobile Devices

Getting rid of your old computer? You can ensure its hard drive doesn't become a treasure chest for identity thieves. Use a program that overwrites or wipes the hard drive many times. Or remove the hard drive, and physically destroy it.

Understand Your Hard Drive

Computers often hold personal and financial information. When you save a file, especially a large one, it is scattered around the hard drive in bits and pieces. When you open a file, the hard drive gathers the bits and pieces and reconstructs them.

When you delete a file, the links to reconstruct the file disappear. But the bits and pieces of the deleted file stay on your computer until they're overwritten, and they can be retrieved with a data recovery program. To remove data from a hard drive permanently, the hard drive needs to be wiped clean.

How to Clean a Hard Drive

Before you clean a hard drive, save the files you want to keep to:

- a USB drive
- a CDRom
- an external hard drive
- a new computer

Consider using a program that overwrites or wipes the hard drive many times; otherwise, the deleted information could be retrieved. Or remove the hard drive, and physically destroy it.

Thinking of upgrading to a new mobile phone or device? Maybe returning one that didn't work out for you? It's important to delete any personal information you stored on the device.

Your mobile device probably holds sensitive information like addresses and phone numbers, passwords, account numbers, email, voicemail, and text message logs. When getting rid of your old device, it's important to take steps to help ensure this information doesn't fall into the wrong hands.

First, try to use the factory reset. Many devices allow you to "wipe" your device and clear nearly all the information in its memory. Sometimes, this is called a "hard reset," or "factory reset." You may be able to save or transfer the information to your new device before you delete it from your old one.