10 A USER'S GUIDE: WAYS TO PROTECT YOUR PERSONAL DATA

1 Don't click that link!

What to do: Don't click links in emails. Instead, type the URL you want directly into the browser.

Why: According to Microsoft, phishing is still the number one favorite method of cyber-attacks.

2 Use two-factor authentication

What to do: Use a second factor for logging into accounts.

Why: If you have a robust two or multi-factor in place, you are much less likely to lose personal data due to phishing.

3 Delete recorded conversations

What to do: Regularly delete any recorded conversations used by your personal assistant.

Why: There have been cases where Alexa revealed personal data to unknown persons without consent.

4 Keep it clean — delete old files

What to do: Make sure you keep data replication to a minimum. Delete old files you don't use.

Why: There can never be 100% security, but reducing the places that can be compromised helps lessen your risk.

5 Be less social

What to do: Minimize the amount of personal data you have on social media platforms.

Why: Information like your pet's name or mother's maiden name is sometimes used to recover account logins. Don't give hackers an easy way into your online accounts!

6 Don't sync for sync's sake

What to do: Disable automatic file and media sharing whenever possible.

Why: A lot of devices set up cloud syncing when you first configure the device. Check if you really want to store these data in the cloud.

7 Keep off the beaten track

What to do: Disable location tracking on each app.

Why: A recent study of almost 1 million Android phones demonstrated that apps regularly harvested tracking data.

8 Let sleeping Bluetooth lie

What to do: If you are not using Bluetooth, switch it off.

Why: Bluetooth vulnerabilities can allow data to be siphoned off your device.

9 Encrypt stored data

What to do: Encrypt any data you store on hard drives and use an email encryption tool if you share personal data.

Why: Encryption is a layer of protection that can prevent lost or stolen data from being exposed.

10 Patch your devices

What to do: Keep your computers and mobile devices patched and up to date.

Why: Software vulnerabilities allow malware to infect your device, which can steal data and login credentials.

Sources

1. Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web, Armor Blog
2. Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, Javelin Research
3. Security Intelligence Report (SIR), Microsoft
4. 2018 Data Breach Investigations Report, Verizon
5. Alexa user gets access to 1,700 audio files from a stranger, TechCrunch
6. Woman says her Amazon device recorded private conversation, sent it out to random contact, KIRO 7
7. Binns, R., et.al., Third Party Tracking in the Mobile Ecosystem, Association for Computing Machinery
8. The Attack Vector "BlueBorne" Exposes Almost Every Connected Device, Armis
9. Breach Level Index, Gemalto

INFOSEC

Top 10 Tips for Password Security

Know your guidelines

Your organization has its own policies for password security. Know them and push them to the limits! If they allow passwords of 8-20 characters, always make it 20.

Longer is better

New research says longer passwords are harder to guess. "Wine" is short; "1998dontdrinkwinewithbadchee$e-2002worstweddingEVER" is long.

Uncommon sense

Substitute uncommon words for common ones. Try to avoid words found in dictionaries, if possible.

Think phrases, not words

A space is just another character in a string, so long phrases with spaces are effectively single unsearchable words. A phrase like "dinosaurs don't dance disco" is unique and memorable!

Choose something only you know

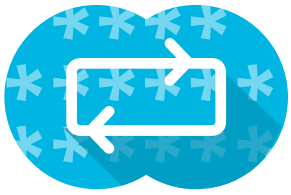
Think of something that makes sense only to you. This could be a private joke, a childhood nickname or an association only you would make.

Don't write it down

Put down the Post-Its! Choose a password you can remember without writing it down. If you absolutely have to write some down, write down a hint that would only make sense to you.

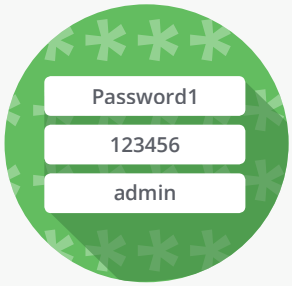
Don't repeat

Don't reuse passwords. If you've already used a password for another account, or used it previously for the same account, invent a new password.



Never share passwords

Passwords are like toothbrushes. Change them regularly and never share them with anyone!



If it hasn't worked before ...

Know your common passwords. "Password1," "123456," "admin" and "qwerty" are all common passwords that hackers will always guess.

Don't use common substitutions

It's become common practice to replace letters with similar-looking numbers and symbols. These are known substitutions and will not help make a password stronger.

Protecting Devices & Media

Top Eight Tips

When it comes to information storage, media can mean anything from computers and hard drives to printouts. Here are some top tips for protecting all forms of devices and information media.

Determine your priorities

Know what devices and media hold the most sensitive information, and stack your priorities accordingly. Some may need more protection than others.

Be familiar with the rules and regulations

Your organization and industry may have special regulations related to information handling. It's important to follow the special rules related to the devices, media and information you deal with.

Encrypt files and devices

Encryption encodes data so that it can't be read without a special password. Even if an attacker steals the whole device, they won't be able to read an encrypted file.

Lock up sensitive information

Media containing sensitive information should be locked up and carefully monitored. Keep a clean desk and don't leave papers or removable drives lying around.

Use strong passwords

Strong passwords are key to protecting devices and the information on them. Use long passwords and passphrases composed of uncommon words.

Keep your system and antivirus updated

An out-of-date device may have security flaws that attackers can exploit. Your software and antivirus should be updated regularly via official updates from the manufacturer.

Keep regular backups

In case of disaster, backups are a lifesaver! Important information should be copiedonto an authorized and secure backup location and stored separately.

Destroy when no longer needed

At the end of the information life cycle, information should be destroyed when no longer needed.

When you're ahead of the game, you can't be gamed.

10 Ways to Be Cyber-Secure at Home

Identify your perimeter

Less is more! The fewer connected devices and entry points you have, the safer your network is.

Update software and devices regularly

Regular updates make you less vulnerable to attack. Only download updates from the manufacturer and enable auto-updates when possible.

Secure your Wi-Fi network

Routers often have default credentials that people don't know about. Disable the "remote configuration" option in your router and change both your Wi-Fi password and your router password.

Watch out for insecure websites

Always use HTTPS for sensitive communications. Don't ignore browser warnings and always remember to check the website address carefully for misspellings and oddly-placed letters or numbers. When in doubt, manually enter the URL in your browser.

Back up your files

Backups save your information if your device breaks or is taken over by an attacker. Back up files to a removable device that can be locked away safely, such as a CD or flash drive.

Don't download carelessly

Files can contain malware, and websites aren't always what they appear to be. Always verify sender identity before downloading files and remember: If it comes from an oddly-spelled email or is hosted on a site that makes your browser generate a warning, stay away!

Encrypt devices to deter thieves

Encryption renders files unreadable without the correct key. Some devices offer the option to encrypt individual files or the entire device. Consider which solution suits your needs best.

Practice password safety

Choose long passwords containing uncommon words. Use unique passwords for sensitive accounts and a password manager to help you remember them.

Always use antivirus software

Antivirus needs updates, too! Set it to auto-update.

Keep yourself informed

New cybersecurity bugs and attacks pop up every week. Staying informed about the latest threats will help you be safe!

INFOSEC

Learn more at infosecinstitute.com

10 Ten Tips for Physical Security

1 LOCK DOWN DEVICES

Place tablets and phones in a locked drawer when not in use. Never leave unsecured devices unattended!

2 USE ENCRYPTION

Many devices will offer the option to encrypt a file or the whole device. Encryption means that even if someone steals the device, they can't read your files.

3 KEEP A CLEAN DESK

Notes, devices and documents can convey sensitive information. Keeping everything locked up and out of sight will help keep that information out of an intruder's hands.

4 PICK UP YOUR PRINT JOBS ASAP

Printouts often contain sensitive information. Be sure to pick up your print jobs right away.

5 DESTROY BEFORE DISCARDING

Documents and electronic files need to be destroyed before the medium itself is thrown out or recycled.

6 DON'T LET PEOPLE FOLLOW YOU IN

Entering the building is the first step for many attackers. Everyone who needs to be there has their own key card; don't let strangers persuade you to let them in!

7 BE AWARE OF SOCIAL ENGINEERING

Social engineers deceive people in order to manipulate them into giving out valuable information or making mistakes. Be aware of the common social engineering tricks, such as pretending to be a delivery person to access a building.

8 BACKUP FILES

Mistakes or accidents will happen, and something will get lost, broken or destroyed. Keeping regular backups will save you from having to redo your work.

9 KNOW GOVERNMENT AND WORKPLACE POLICIES

Your industry may fall under special government regulations for physical security. It's important to know the policies that apply to your situation, whether they were put in place by the company or the government.

10 KEEP AN EYE OUT

Be aware of your surroundings. Intruders may eavesdrop or spy on you over your shoulder! If entering a PIN on a pad, shield the pad with your hand.

Knowledge is your best defense.

Recognize and Combat Social Engineering

CYBERCRIMINALS

Want access to something sensitive

They want your boss's information or the number of an account, or even want to get into the building. Stand firm and ask for proof of identification.

Exert pressure on you

Social engineers want you to act without thinking. If someone is pressuring you to do something without giving you time to consider it, that's a sign of a social engineer.

Send offers too good to be true

You've won the lottery! Or not. If an offer or opportunity seems too good to be true — it probably is.

Pretend to be a client or authority figure

Social engineers will impersonate clients, bosses, friends, family or others who may be able to influence you. Always take extra steps to prove their identity!

Are unwilling to prove identity

A social engineer will often deflect or get angry when asked to prove their identity. They may try to stop you from contacting other people for verification or refuse to give proof.

YOU

Examine all links and attachments

You may receive innocent-looking links or attachments which actually contain malware; examine carefully and don't click unless you're certain it's safe.

Don't use their contact methods

If a message might be from an impostor, contact the real person or organization through a known, safe method, such as a public phone number.

Escalate

If someone's story sounds fishy or they can't prove who they are, pass the issue — and your concerns — up the chain of command.

Don't let yourself be bullied

Social engineers may try to intimidate, emotionally blackmail or threaten you. Don't let it faze you.

Don't share information an attacker could use

If you share personal or sensitive information online, an attacker can harvest it for use in impersonation or attacks.

10 Tips for Spotting SMiShing and Vishing

Look out for social engineering

The attacker's goal is often to convince you to talk to them so they can trick you into sharing sensitive information.

Be aware that urgency is a red flag

Attackers want you to react fast, without thinking about the consequences. Their phone calls and texts are made to provoke — claiming importance, danger or disaster.

Don't use their contact methods

If you suspect SMS phishing or voice phishing, don't contact them back using the methods they provide. Use an official phone number or website.

Remember that your phone can get malware

Getting malware onto your phone is one way attackers may breach a network. Always have antivirus on your mobile device!

Don't assume automated calls are legitimate

Some attackers will use text-to-speech devices or voice filters to sound like the automated calls used by legitimate organizations. Never assume a call is legitimate because it sounds automated.

Remember that caller ID is not foolproof

Attackers are capable of spoofing caller ID to fool their targets. Never rely on caller ID alone to prove identity.

If you suspect SMiShing or vishing, report it immediately

SMiShing and vishing can lead to holes in the overall security network and result in major breaches or losses. Always report suspected attacks to your supervisor.

Look out for common attacks

Fake security notifications and messages from government agencies are two common forms of SMiShing attacks. Vishers may impersonate government agencies, bill collectors, banks and others.

Don't click on links or download any software updates or apps from texts

Updates will never arrive via text message! Never click on a link in a text. Use a search engine or a bookmark to navigate to the site instead.

Don't show your hand

Keep your cards close to your chest. Never reveal sensitive information to someone who has called you. Call the organization back via an official number in order to fulfill information requests.

10 Tips to Recognize & Prevent Insider Threats

THEM

Are malicious OR misguided

Internal breaches can be intentional or unintentional. Insider threats can be malicious (deliberately causing damage) or accidental (making mistakes, forgetting to secure something or otherwise accidentally causing damage).

May be anyone

It's not just the everyday employees or higher-ups! An insider threat may be a contractor, a consultant, a vendor or a former employee.

Act out of the ordinary

They seek to work unusual hours, ask for access to restricted information or brag about sudden, mysterious financial windfalls.

May have different motivations

Money may not be the only obvious motivation. Malicious insiders may be motivated by perceived slights, political or religious leanings, job dissatisfaction or revenge.

Violate policies

Insiders violate policies by definition, either knowingly or unknowingly. Policies are put in place to protect customers, data and the company, and an insider's damage to the company will violate those policies.

YOU

Know and follow security procedures

Accidental insiders can cause breaches not through malice, but because they make mistakes. Following established procedures, and noticing when procedures aren't followed by others, can prevent potential mistakes.

Report suspicious behavior

If someone is acting suspicious or dangerous, management needs to know. Share your concerns with your supervisor. By reporting small signs, you could stop a problem before it becomes a disaster.

Trust but verify

If you suspect someone is an insider, be cautious. Verify their claims and maintain security until you can be certain of the situation: never share your password or access with a potential insider.

Practice good physical security and cybersecurity

Maintain a clean environment, lock up sensitive documents and password-protect and encrypt important files.

Know the signs of a disgruntled employee

Is someone picking fights with coworkers or angling to get fired? A disgruntled employee is one who may become an insider threat.

INFOSEC

Learn more at infosecinstitute.com