Own IT. IT’s up to you.

Who wants to know?

There’s more than three billion people on the internet, and not all of them are who they say they are. Keep your friends list small, and never friend anyone you don’t know in real life.

The internet never forgets

With archive sites, screencaps and the quick spread of information on social media, the internet never forgets a mistake. You may dance like nobody’s watching, but post like everyone is.

Sharing is not caring

It’s tempting to share everything about your life, but what you share can be used by someone else. With that information, an attacker can impersonate you or break into your accounts on different sites.

Take it slow

Attackers will often goad people into making quick decisions, hoping to take advantage of your mistakes. Think fast, but type slow, and they can’t touch you.
Own IT. IT’s up to you.

A few **good** friends

The best way to keep yourself and your information safe is to **limit your friends list** and restrict what you post to your friends only.

**Friendbook**

<table>
<thead>
<tr>
<th>Friends</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stacy Kingly</td>
</tr>
<tr>
<td>Georgie Red</td>
</tr>
<tr>
<td>Daryl Wentz</td>
</tr>
</tbody>
</table>

**Bad share day**

When you log into an account with a third-party app or service, information is being shared between that service and your account. **Keep a lid on your data** by using your individual login and not installing extensions.

**Location unknown**

If your location is known and being tracked by the phone in your pocket, then apps with that permission can access that data and follow you. **Keep yourself hidden** by turning off your location data.

**Syncing ship**

Disabling auto-sync forces someone who’s stolen your account or device to enter your password, which will stop an attacker who doesn’t know it.

**Lockdown**

A lock screen saves a lot of trouble in the long run. Even if your device is stolen, the attacker likely won’t know your password. **Enable encryption** so that even if the lock screen is subverted, the data is still inaccessible.
Own IT. IT’s up to you.

Beware permissions
When you install an app, what permissions does it ask for? A tracking app may want to know your location, but a beauty app doesn’t need that information. Never give network permissions to anything that doesn’t need it.

Allow Candy Kracker to take pictures, make recordings and access your calendar, photos, files, contacts, microphone, sensors, storage, call logs and search history?
DENY  ALLOW

Source smart
Whenever possible, choose apps from a reputable creator and download only from the official app store.

Vaccinate your device
Every device needs an antivirus. Even if you end up downloading a dangerous app, or a previously safe app becomes infected, an antivirus will help to secure the device.

Spot the scam
There are several signs that an app might be a scam or a disguised attack. If it has a lot of five-star ratings but no reviews, it could be a scam. If the creator is suspiciously silent or refuses to promote their app, then you should be cautious.

Make Quik Cash
Free Cash App!
Connect to your bank and make money NOW!
5-star | 0 reviews
Install now

© 2019 Infosec. All rights reserved.
Longer and stronger
Shorter passwords are easier for hackers to break. NIST, the National Institute for Standards and Technology, recommends that passwords be anywhere from 8 to 64 characters long.

Mix and match
Do you like mixing languages or making up your own words? If so, then you have an easy way to improve your password. **If it only makes sense to you**, it’s less likely to appear in the cracked lists of passwords hackers use.

Ditch the digits?
While your own organization's rules may be different, new federal guidance has advised that forcing users to include lots of symbols and numbers doesn't necessarily increase password security. **Focus on length and memorability** instead.

Thinking in sentences
How do you remember a password that's 64 characters long? Think in sentences, not words. A phrase or a sentence is easier to recall than a nonsensical combination of letters and numbers, and provides that all-important length to make it harder to crack.

```
jst4sm4lt0wngrl!lvnngen4l0nelyw0rld!!
t00kth3mdnghttr4ng0ng4nwh3r33!!!
```
Secure IT. IT’s up to you.

**Two locks are better than one**

Having two or more authentication steps makes it harder for attackers to breach an account. Most apps, devices and services have the option to **enable multi-factor authentication**, and it’s always smart to use it.

**To have and have not**

There are three different types of authentication: what you know, what you have and what you are. Mixing authentication types will give you **stronger protection**. If someone has stolen your password but not your cell phone, they’re out of luck!

The **eyes** have it

Biometric authentication, the “something you are” factor, can be anything from a signature match to a fingerprint, palm or even iris scan. Consider implementing biometrics to provide an **extra layer of security**.
Secure IT. IT’s up to you.

Don’t reuse passwords
Passwords get cracked all the time, and each broken password is added to a hacker’s database of passwords to use in the future. Always use unique passwords.

Link and you’ll miss it
Links on websites and in emails can be spoofed, making you think you’re going to a site you aren’t. Instead, use bookmarks to ensure you’re going right back to where you want to be.

Spot the scam
A product or service may look good on the site, but how do you know it’s legitimate before you buy? Consumer watchdogs like the Better Business Bureau can help you check if a business is on the level — before you give them your credit card number.

Look for the S
These days, a legitimate shopping site is going to be using HTTPS rather than HTTP. (The S stands for “secure.”) Look in the upper corner of the screen for the HTTPS and the lock icon.

© 2019 Infosec. All rights reserved.
Secure IT. It’s up to you.

Friend or foe?

Phishers want to get their hooks into you as fast as possible. If someone is too eager to be friends and to offer you a great opportunity, you could be smelling something phishy.

Hey I spoke to Lisa yesterday and she said I should contact you directly. Send me a friend request so I can transfer you that money now.

Slow and steady

If someone is pressing you to do something right now, slow down the interaction. Ask more questions and consult people you trust. If you can’t confirm that it’s legitimate, pass it on for a second opinion.

Phish fight

Play hard to get! Don’t download anything you suspect might be dangerous, and don’t send a questionable contact the information they ask for.

Too good to be true

Phishers want you to make mistakes, and they’ll offer you amazing deals or quick money to get you to make that careless choice. Ask yourself: is this too good to be true?

CONGRATS!!
You won the lottery.
Please go here to claim.

© 2019 Infosec. All rights reserved.
Protect IT. IT’s up to you.

Always update
Updates fix bugs, patch insecurities and keep your programs and devices running smoothly. Remember, the criminals are updating their attack methods.

Source matters
Only download software updates from official sources. If you don't have the option to automatically update, check the manufacturer’s site for updates and patches; don’t trust browser warnings asking you to download things.

Click attack
A fake warning will ask you to download a file or fill in a form, but a real browser warning will only ask you to not do something: don’t click ahead, don’t stay here.

License to fail
Never use cracked, pirated or unlicensed versions of software or an OS; these often contain malware and cause more problems than they solve.

Shield your system with auto-update
Legitimate programs will often give you the option to enable auto-update. With this, the software will automatically download updates and patches when they become available, taking the stress of updating off your shoulders and ensuring that you’re running the latest versions.

© 2019 Infosec. All rights reserved.
Public has **no privacy**

Using **public networks is always a risk**. When using a public network, such as in a coffee shop or an airport, never access private information like your bank or your email.

**Auto-connect is not correct**

Having a device automatically connect to known and remembered networks is a fast ticket to malware. **Disable auto-connect** and carefully choose the network you want.

**Password preferred**

Public, unprotected networks are more likely to be run by hackers looking for an easy target. When working remotely, always **use the password-protected networks** controlled and monitored by the business owner.

**Spot the copycat**

Hackers will sometimes create copycat networks with the same or similar names to existing, legitimate networks. These copycats will lack password protection to entice people into using them. When connecting to a network run by a person or a business, **always confirm** exactly which network is theirs and whether it’s supposed to be password-protected.
Protect IT. IT’s up to you.

Less is more
The less data you have on hand, the less can be lost in the event of a data breach and the less danger for the customer.

By the book
It's important to know the policies for handling customer data and be familiar with your role in an emergency.

Sharing isn’t caring
Never let someone else access sensitive data unless they are explicitly authorized and their identity has been proven. Impostors may try to tell you a good story, but that data represents a person’s life and safety.

Lockdown
Customer information needs protection. Physical copies should be locked up in a secure location; digital information should be encrypted and kept under strong passwords.

Who goes there?
You need strong physical security to protect data as well: locks, badge checks and confirming that personnel are authorized to access the area.

Shred and buried
When customer data is no longer needed, the records should be destroyed. Papers should be shredded or pulped, and devices storing electronic records thoroughly erased.