How to create a cyber secure home

October 5 2017

Credit: Ohio University

As technology becomes more important in our personal lives, so does securing it. Here are some fundamental steps you should always take to help protect yourself and your family.

Securing yourself

Cyber attackers have learned that the easiest way to get something is to simply ask for it. As such, common sense is your best defense. If a message or phone call seems odd, suspicious, or too good to be true, it may be an attack.

Securing your home network

Your WiFi router is a physical device that controls who can connect to your wireless network at home. Follow these steps to secure it:

- Always change the default admin password on your router to a strong password only you know.
- Configure your network so that if anyone wants to join it, they have to use a password. In addition, always configure your network to use the latest encryption, which is currently WPA2.
- Be aware of all the devices connected to your network, including baby monitors, gaming consoles, TVs, or perhaps even your car.

Securing your computers and devices

- Protect your devices are protected with a strong PIN or passcode and are running the latest version of their software.
- Enable automatic updates whenver possible.
- If you can, have two computers at home, one for parents and one for kids. If sharing a computer, make sure everyone has separate accounts and that kids do not have privileged access.
- Use a firewall and anti-virus on your computers.
- Before disposing of a device, make sure it has been wiped/factory reset.

Securing your accounts/passwords

- Always use long passwords that are hard to guess. Use passphrases where possible - passwords with multiple words, like "Where's my coffee?"
- Use unique passwords for each account and device. Can't remember that many? Use a password manager app to keep track of them for you.
- Use two-step or multi-factor authentication whenever possible. This adds a personalized step to logging in, like receiving a text or phone call on your mobile phone.
- On social media, post only what you want the public to see. Assume anything you post will eventually be seen by your parents or boss.

What to do when hacked

No matter how secure you are, sooner or later, you may be hacked:

- Create regular backups of all your personal data. If a device gets hacked, the only way to recover its data may be from a backup.
- If one of your online accounts has been hacked, immediately log in and change its password to a strong, unique password. If you no longer have access, contact the company.
- Monitor your credit cards. If you see charges you do not recognize, call the company right away.

Provided by Ohio University

Citation: How to create a cyber secure home (2017, October 5) retrieved 20 April 2024 from https://phys.org/news/2017-10-cyber-home.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.