View as Webpage

Your Smart Devices Are an Invitation to Hackers

In today's connected world, smart devices have become ubiquitous, and have enhanced our daily lives with convenience and efficiency. However, they also pose significant security risks.

There are countless stories of home security cameras being hacked. Recently, a family was targeted by a hacker who cranked up their smart thermostat to unbearably high temperatures. In another incident, a couple woke up to a stranger inappropriately talking to their infant through a baby cam and monitor. Even more alarming, a scammer managed to hack into an office's fish tank sensors, gaining access to the company's computer systems and stealing a treasure trove of data.

You might be thinking, "That would never happen to me." Yet, the average home or office, with all its internet-connected devices, experiences about 10 attacks every 24 hours. Everything from your smart light bulbs to your smart thermostat is a potential entry point for hackers. While you don't need to ditch your smart gear, it's essential to know how to protect your home and office effectively.

Common Hacker Attacks

Smart devices, collectively known as the **Internet of Things (IoT)**, introduce new vulnerabilities. These modern conveniences often have overlooked or downplayed security issues. It's hard to imagine a fish tank as a security threat, but many seemingly harmless smart devices pose risks if not secured properly.

Here are some common types of cyberattacks on smart devices:

- **Botnet Recruitment:** Hackers can add your devices to an army of infected devices, using them to carry out larger attacks.
- **Data Theft:** Many smart devices collect personal details like location, behavior, and health data, which are valuable on the dark web.
- **Spying:** Hackers can listen in, watch, record, or steal information to bolster future attacks.
- **Cryptojacking:** Thieves use your computer's processing power and internet connection to mine cryptocurrency.

The Security Issues with Cameras

Security cameras are particularly vulnerable to cyberattacks. Wi-Fi cameras, connected to the internet, are the most at risk. Even if hackers can't get a direct connection to the camera, they can gain access through cloud-based servers. Unfortunately, many security camera systems are easy to hack because users often do not change the default username and password or their credentials become compromised.

The Problem with Printers

Modern home and office printers, connected to the internet, present significant security risks. In 2023, 61% of organizations experienced data loss through their printers. These multi-function printers can provide a direct path into your computer systems, allowing hackers to inject malware, disrupt other devices, steal data, and launch attacks.

Protecting Your Network

Windows PCs and Macs both have built-in firewalls. Ensure these are enabled on your devices:

- **On Windows:** Open Control Panel, type "firewall" into the search box, click Windows Defender Firewall, and in the left pane, tap "Turn Windows Defender Firewall on or off."
- **On Mac:** Click the Apple menu > System Settings > Firewall, then turn it on.

How To Protect Your Smart Devices

Basic Security Measures:

- **Use Strong Passwords:** Create strong, unique passwords for your Wi-Fi network and all smart devices. Avoid using default passwords.
- **Enable Encryption:** Ensure your Wi-Fi network uses WPA3 encryption to protect transmitted data.
- **Set Up a Guest Network:** Create a separate guest network to prevent visitors from accessing your main network and connected devices.

Monitor Device Activity:

- **Check Logs:** Regularly review device logs and network activity for unusual access attempts.
- **Use Security Software:** Install reputable security software on smart devices to detect and prevent malicious activities.

Educate Yourself and Others:

- **Stay Informed and Raise Awareness:** Follow trusted

Keep Devices Updated:

- **Install Updates:** Regularly update the firmware and software of your smart devices to patch security vulnerabilities.
- **Enable Automatic Updates:** Enable automatic updates to ensure devices are always running the latest security patches.

Implement Two-Factor Authentication (2FA):

- **Enable 2FA:** Use two-factor authentication for device access and associated online accounts for an extra layer of security.

Disable Unused Features:

- **Turn Off Unnecessary Functions:** Disable features such as remote access, microphones, and cameras when not in use.

cybersecurity news sources and organizations to keep up-to-date with the latest threats and educate family and employees about smart device security.

For additional security information, you can visitOak Bank's Security Information on our website.

Need help with your account?

Email: bank@oak.bank
Call: 608.441.6000

- If your Oak Bank Debit/ATM Card has been misplaced, call 877.755.2957.
- If you have misplaced your Oak Bank Visa Credit Card, call 800.423.7503.

VISIT OAK BANK ONLINE

608.441.6000
877.625.2265 Toll Free

Lobby
M - F: 8 a.m. - 5 p.m.

Drive-up
M - F: 8 a.m. - 5 p.m.

Member FDIC

Oak Bank NMLS #434669

Oak Bank | 5951 McKee Road, Suite 100 | Fitchburg, WI 53719 US

Unsubscribe | Update Profile | Our Privacy Policy | Constant Contact Data Notice