

[View as Webpage](#)

What is patching and why should you do it?

Patching and software updates are important components in maintaining a high level of security. By staying on top of patches and updating your operating systems, internet browsers, apps, and plugins on your computers and mobile devices, you are protecting yourself from unwanted parties obtaining access.



What is patching?

According to the [Cybersecurity & Infrastructure Security Agency \(CISA\)](#), patches are software and operating system updates designed to address any security vulnerabilities within the programs on your computer or mobile device. In addition to security updates, patches also address improvements in technology or productivity to ensure your programs and devices are running at the best of their abilities.

How often should you look for patches or updates?

Some programs will run automatic software updates, and some will require you to take action. Frequently check for updates on vendor websites, as attackers become aware of vulnerabilities and use them to exploit security loopholes.

Types of Updates:

- **Manual:** Requires the user or system administrator to take action by downloading patches or software from the vendor website.
- **Automatic:** Consent is provided at the time of downloading or purchasing the product, and automatic updates and patches are pushed to your software or device as they are available.

Patching Best Practices:

- Set up automatic updates on your computers or mobile devices whenever they are available. This allows for peace of mind that your devices and programs are always functioning properly and securely.
- Avoid using **end-of-life (EOL) software**.
- Make sure you're visiting the vendor's website directly vs. entering through a third-party source (email, ads, etc.) Even if the ad or email appears trustworthy, you can eliminate any potential problems by visiting the site directly.
- Never update your computer or mobile devices while on untrusted or public networks.



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



Oak Bank will never ask for personal information over an unsolicited phone call, text, email, or online chat. Never share your account information, PIN number, username/password or one-time password.

If you receive an unsolicited phone call or text message requesting your Oak Bank account information, report it immediately by calling 608.441.6000 or sending an email to bank@oak.bank.




Need help with your account?


Email: bank@oak.bank
Call: 608.441.6000


If your Oak Bank Debit/ATM Card has been misplaced, call 800.472.3272.

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.



STAY CONNECTED



This Oak Bank message may contain promotional content.

Oak Bank | 5951 McKee Road, Fitchburg, WI 53719

[Unsubscribe kvirnoche@oak.bank](#)

[Update Profile](#) | [Constant Contact Data Notice](#)

Sent by noreply@oak.bank powered by



Try email marketing for free today!