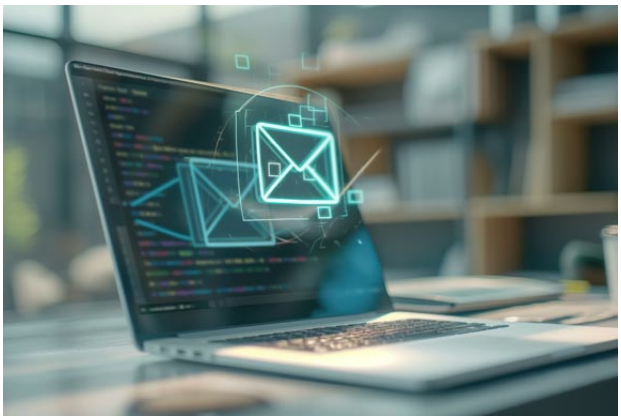
View as Webpage

Understanding Email Takeovers Helps You Stay Protected



An **email takeover** happens when a cybercriminal gains access to your email account—often without you even knowing. Once inside, they can impersonate you, steal sensitive information, or launch further attacks.

Here's what you need to know—and how to protect yourself.

How Email Takeovers Happen

1. Stolen Login Details

- **Phishing:** Fake emails or websites trick you into revealing your username and password.
- **Credential Stuffing:** If you reuse passwords across accounts, attackers can use leaked info from other sites to access your email.
- **Malware:** Some viruses (like keyloggers) secretly track what you type and send it to attackers.

2. Testing the Access

Once criminals get your credentials, they test them—either manually or using automated bots. If successful, they may:

- Send spam or phishing emails
- Steal your personal or financial info
- Lock you out of your own account
- Try to scam your contacts

How to Stay Protected

Use Strong, Unique Passwords

- Use unique passwords across sites.
- A password manager can help you create and safely store complex passwords.

- **Turn On Two-Factor Authentication (2FA)**
  - Add an extra layer of security with a code sent to your phone or an authentication app.
- **Stay Alert with Email Security**
  - Don't click links or open attachments from unknown senders.
  - Double-check email addresses—especially if an email seems urgent or asks for money.
- **Keep Your Software Updated**
  - Make sure your operating system, email app, and antivirus software are up to date.
- **Use Safe Connections For Secure Browsing**
  - Avoid logging in on public Wi-Fi. If you must, use a VPN to encrypt your connection.
- **Monitor Account Activity**
  - Check for unexpected logins or setting changes.
  - Watch for security alerts from your email provider.
- **Add Extra Protection**
  - Use spam filters.
  - Use a second email address for things like online shopping or newsletters.
  - Limit how much personal info you share publicly.

By taking these simple steps, you can greatly reduce your chances of falling victim to an email takeover.

If You Think You've Been Hacked

- **Change your email password right away**
- **Run a virus/malware scan** on your devices
- **Let your contacts know** your account may be compromised
- **Report it to your email provider**
- Consider **identity theft protection** and **creating a new account**, if needed

For additional security information, you can visit Oak 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