



Safeguard Your Online Holiday Shopping Experience

As you shop for your holiday gifts, the appeal of online shopping is undeniable. Convenience and enticing discounts make it an easy way to get the perfect gift for everyone on your list. In the spirit of ensuring a secure and enjoyable holiday season, we'd like to share some information that will help you safeguard your online shopping and protect your personal information.

Watch Out for Phishing Scams

Phishing is one of the most common scamming techniques. Emails, usually that prey on your emotions, encourage you to take immediate action of some kind. Hackers use ploys like saying you're a "big winner," or that your account will close immediately if you don't do something.

In the first few weeks of November, security experts at Egress identified a staggering 237% surge in phishing emails related to Black Friday and Cyber Monday.

securityMETRICS

7 Signs of a Phishing Email

The diagram shows a simulated phishing email interface with seven numbered callouts pointing to specific red flags:

- 1** Sir/Madam, (Generic greeting or no greeting at all)
- 2** You are required to use [this form](#) to update your login information immediately. (Request for personal information over email)
- 3** [CLICK HERE NOW!](#) (Buttons with hyperlinks to unfamiliar webpages)
- 4** [unsolicited.pdf.exe](#) (Unsolicited attachments)
- 5** Manager <manager@fakeco.com> (From email address is not official)
- 6** [fakeweb.com](#) (Hover your mouse to reveal misleading URL hyperlinks)
- 7** (Spelling and grammar mistakes)

© 2020 SecurityMetrics

Follow these safety measures against phishing scams:

Watch out for:

- Appealing holiday specials that seem too good to be true.
- Shipping or delivery issues for supposed packages.
- Fake invoices or notifications for unauthorized purchases.
- Offers for heavily discounted gift cards.
- Phony charity websites and emails seeking donations.
- Suspicious email names, especially with misspellings or extra characters.

If you suspect a scam:

1. Do not respond to the email or click any links. Immediately mark it as junk or spam and block the sender. (For phone calls, hang up!)
2. If your banking information is compromised, give us a call immediately at 608.441.6000.
3. Change the password to any accounts that might have been compromised.
4. Implement multi-factor authentication on your logins wherever possible.
5. Keep security software on your devices updated.

Other Scams to Avoid:

- **Typosquatting Scams:** a scam that utilizes typos in the URL of a website to make you think it's a real store. For example, amazon.com instead of amazon.com. Use only reputable websites and double-check the URL.
- **Gift Card Scams:** enticing offers of free gift cards, which are often an attempt to get your personal information.
- **Charity Scams:** fake charities set up to steal donations; most charities won't take donations through cryptocurrency, wire transfers or gift cards so especially be careful of these donation methods.
- **Package Delivery Scams:** fake delivery notifications, calls or texts that lead to fake websites.
- **Fake Gift Exchanges:** online gift exchanges that resemble pyramid schemes where you send a gift to someone you've never met and will in turn receive a gift.
- **Emergency Scams:** emergency-related requests for money, even from friends or family. Hang up the phone and verify with the person that they made the request.
- **Fake Pet Purchases:** fake sellers take your money in exchange for a puppy or other pet without delivery.

Online shopping is a convenient way to check off everything on your holiday list this year. Just remember to be careful and protect your information so it's not used for fraud. Please call 608.441.6000 with any questions or concerns you might have.

What do you do if you see a discrepancy or suspect fraud on your bank account?

1. Contact ALL your financial institutions, not just the account that has the issue.
 2. Have the financial institution freeze the fraudulent account(s).
 3. Place a credit fraud alert on your credit report.
 4. File a report with the Federal Trade Commission.
 5. File a report with the police.
 6. Continue to monitor ALL your other accounts for discrepancies.
-

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 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.



Oak Bank NMLS #434669



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

[Unsubscribe kvirnoche@oak.bank](mailto:kvirnoche@oak.bank)

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

Sent by noreply@oak.bank powered by



Try email marketing for free today!