Phishing

What is Phishing?

Criminals use malicious email and websites to try to trick you into revealing your password or other sensitive information or to infect your computer with malware. Phishing email often uses urgent language, asks for personal information, and has grammatical, typographical, or other obvious errors.

By tricking Oakland Schools' users into giving away their information, attackers can:

- Steal money from victims (modify direct deposit information, drain bank accounts)
- Perform identity theft (run up charges on credit cards, open new accounts)
- Send spam from compromised email accounts
- Use your credentials to access Oakland Schools systems with financial, student or other confidential information.

Review the following resources to learn how to protect yourself and how to report suspicious communications.

What can I do about it?

If you have given personal information in response to a phishing email or on a suspicious webpage, **your account may be compromised.**

Change your password and report suspicious emails you receive to your Oakland Schools account. You can do this by forwarding the e-mail to: SPAM@oakland.k12.mi.us

Anti-Phish Tips

Never send your password in email

THE TRAP: You receive an urgent email that appears to be from the Oakland Schools Service Desk asking you to reply with your password because your account is "compromised" or "over quota" or "suspended due to inactivity".

YOUR DEFENSE: Oakland Schools and organizations that care about the protection of your information should never ask you to send bank account numbers, Social Security Numbers, driver's license numbers, health information, or health insurance information via email. Decline requests to send this information in email.

Don't click unexpected links

THE TRAP: You receive an unexpected email that claims to be from the "Help Desk" or someone you know. It says it's urgent. You must click a link to prevent problems with your account.

YOUR DEFENSE: Be skeptical of any email that you aren't expecting. Password thieves may insist that immediate action is necessary and may pretend to be your friend or some other trusted entity. Don't let these tactics trick you into letting down your guard. It is very likely a scam.

Look out for deceptive links

THE TRAP: You receive an email telling you to "click here" to verify your account.

YOUR DEFENSE: Hover over the link (don't click!), or for a touchscreen, press and hold the link (don't tap!) to reveal the actual URL. (Look in the bottom left corner of the browser window.) Don't click on a link unless it goes to a URL you trust.

Check link to protect your password

THE TRAP: You are asked to enter your Oakland School password on what looks like the standard Google or webmail page.

YOUR DEFENSE: Always check the actual URL to make sure it starts with HTTPS:// and is from a domain you trust. Fraudulent login screens designed to steal your credentials may LOOK authentic if you're not paying attention to the URL.

Trust your instincts and verify requests

THE TRAP: You receive an email from someone you trust but something just isn't right. For example, your manager wants you to send a check to a company you haven't heard of before.

YOUR DEFENSE: Verify the message you received by communicating with the the sender in person or with a phone call. For additional help forward the message to SPAM@oakland.k12.mi.us and servicedesk@oakland.k12.mi.us for assistance in determining if a message is a phishing message.

Additional Resources

If you'd like to get further information on how to avoid bad actors from getting their hands on your data, see the links below.

Google Phishing Quiz

Can you spot when you're being Phished? Try this quiz to see how prepared you are!