TOBIN
SOLUTIONS

So, You Got Phished! What is Phishing?

A Better Technology Experience

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

What Do I Do?

1. Notify your manager or supervisor or IT manager
2. Alert the rest of your company of the phishing attack to limit or prevent a breach by others
3. Call Tobin Solutions for immediate assistance – **414-443-9999**
4. Review and follow your security incident response policy plan
5. If you are already using two-factor/multi-factor authentication, you may be safe for this site. If you aren't currently using it, consider enabling it to reduce the impact. Note that even with this enabled, the password is considered breached and should be changed.
6. Do not install any software recommended by the attacker. Please notify your IT provider if you installed any software related to the phishing attack. If software has been installed or modified, it's recommended to wipe your hard drive
7. Change your password and ensure it is long and complex
8. If you have re-used this breached password with any other web services or system, change it now
9. If this is banking related, notify your bank
10. If this is credit card related, notify your credit card company
11. If this involves wire fraud, notify the parties involved and the banks involved
12. If this involves wire fraud or ransomware, contact the FBI
13. Do you need to contact your insurance company?
14. Do you need to preserve evidence?
15. Run a full virus/malware scan of your computer
16. For the affected web service, where possible have your IT provider check:
    a. Log in attempts by your account
    b. Any possible system changes like email forwarding rules
    c. Check other accounts for anomalies
17. If log in attempts were successfully made by the attacker
    a. Look for any data that has been forwarded or extracted from the system
    b. Determine the scope of the breach and create a course of action appropriate to your business needs
18. Update the new password on other devices like your smartphone or tablet
19. Test to make sure you can access your system using the new password
20. Update your cybersecurity awareness training
21. For the next week, monitor your systems for any anomalous or strange behavior and contact Tobin Solutions to report anything suspicious