Phishing

place your
+
logo here

10 steps to identify and handle a phishing email

Phishing is used by cyber criminals to steal passwords and sensitive information, or to infect computers with malware. The attacker poses as a trusted person or organization, to trick the victim to take an action. Phishing can be very dangerous and should be taken seriously.

1 Don't trust the senders display name

Display names can be spoofed. Be sure to always take a close look at the senders email address. Make sure the spelling of the domain is spelled right.

2 General / unfamiliar salutation

Be careful when the salutation is impersonal. This could be a indicator for a mass targeting phishing campaign.

3 Don't click on links and pictures

Don't klick on hyperlinks you don't trust. Hyperlinks can be easily spoofed. Try to hover the link, without clicking, to show the real destination.

4 Don't open attachements

Don't open attachements that you're not waiting for. Word or Excel documents my contain malicious code and infect your computer.

5 Spelling mistakes / Bad language

Attackers often speak different languages than their targets. If there are a lot of spelling mistakes or bad language it's most likely phishing.

6 Be careful about urgency

Attackers may try to set you under pressure. This is a trick to force you into an action without thinking. Always take the time you need.

7 Check if the signature seems valid

Check if there is a signature und be sure that it's a valid signature like the ones you use in your company.

8 Asking for sensitive information

Don't answer questions for sensitive information, when your not sure about the sender. No serious actor will ever ask for your password!

9 Don't trust everything

Always question the content of emails. Attackers often lie to gain your trust. If it's too good to be true, it's most likely phising.

10 In doubt, contact the SOC

If your not sure if an email is valid or not, report it to your SOC or IT (security) department. It's always better to be safe than sorry.

Phishing

place your
+
logo here

10 steps to identify and handle a phishing email

Phishing is used by cyber criminals to steal passwords and sensitive information, or to infect computers with malware. The attacker poses as a trusted person or organization, to trick the victim to take an action. Phishing can be very dangerous and should be taken seriously.

1 Don't trust the senders display name

Display names can be spoofed. Be sure to always take a close look at the senders email address. Make sure the spelling of the domain is spelled right.

2 General / unfamiliar salutation

Be careful when the salutation is impersonal. This could be a indicator for a mass targeting phishing campaign.

3 Don't click on links and pictures

Don't klick on hyperlinks you don't trust. Hyperlinks can be easily spoofed. Try to hover the link, without clicking, to show the real destination.

4 Don't open attachements

Don't open attachements that you're not waiting for. Word or Excel documents my contain malicious code and infect your computer.

5 Spelling mistakes / Bad language

Attackers often speak different languages than their targets. If there are a lot of spelling mistakes or bad language it's most likely phishing.

6 Be careful about urgency

Attackers may try to set you under pressure. This is a trick to force you into an action without thinking. Always take the time you need.

7 Check if the signature seems valid

Check if there is a signature und be sure that it's a valid signature like the ones you use in your company.

8 Asking for sensitive information

Don't answer questions for sensitive information, when your not sure about the sender. No serious actor will ever ask for your password!

9 Don't trust everything

Always question the content of emails. Attackers often lie to gain your trust. If it's too good to be true, it's most likely phising.

10 In doubt, contact the SOC

If your not sure if an email is valid or not, report it to your SOC or IT (security) department. It's always better to be safe than sorry.

Phishing

place your
+
logo here

10 Schritte gegen Phishing

Phishing wird von Kriminellen genutzt, um Passwörter und sensible Daten zu stehlen, oder um Computer mit Schadsoftware zu infizieren. Die Angreifer geben sich dabei oft als vertraute Person oder Organisation aus, um das Opfer zu einer Handlung zu bewegen.

1 Vertrauen Sie nicht dem Anzeigenamen

Anzeigenamen können gefälscht werden. Prüfen Sie immer genau die E-Mail Adresse des Absenders. Auf Schreibfehler in der Domain achten.

2 Allgemeine / unpersönliche Anrede

Phishing Mails verwenden oft allgemeine Begrüßungen. Auch ungewöhnliche Grußformeln können ein Indiz für Phishing sein.

3 Nur schauen, nicht klicken

Hyperlinks können leicht manipuliert werden. Schauen Sie sich das Ziel eines Links genau an, bevor Sie es öffnen.

4 Anhänge nicht blind öffnen

Öffnen Sie keine Anhänge, welche Sie nicht erwarten. Auch Word, Excel und PDF Dateien können Schadcode enthalten, um Ihren Computer zu infizieren.

5 Rechtschreib- und Grammatikfehler

Phishing Mails enthalten oft Schreibfehler, da sie in fremder Sprache geschrieben und anschließend übersetzt werden.

6 Dringlichkeit und Zeitdruck

Wenn Sie aufgefordert werden, in einer kurzen Frist zu handeln, sollten Sie stutzig werden. Besonders in Verbindung mit Drohung von Konsequenzen.

7 Prüfen Sie die Signatur

Prüfen Sie ob die Signatur einer E-Mail dem gewohnten Schema entspricht. Falls nicht, kann dies ein Indiz für Phishing sein.

8 Die Frage nach sensiblen Daten

Angreifer fragen gezielt nach sensiblen Daten. Kein seriöser Absender wird Sie jemals nach Ihrem Passwort fragen.

9 Zu gut um wahr zu sein

Hinterfragen Sie stets den Inhalt einer E-Mail. Angreifer lügen oft um Ihr vertrauen zu gewinnen. Ist es zu schön um Wahr zu sein, ist es wahrscheinlich Phishing.

10 Im Zweifel die IT kontaktieren

Better safe than sorry! Im Zweifel wenden Sie sich immer zuerst an Ihre interne IT oder IT-Sicherheit.

Phishing

place your
+
logo here

10 Schritte gegen Phishing

Phishing wird von Kriminellen genutzt, um Passwörter und sensible Daten zu stehlen, oder um Computer mit Schadsoftware zu infizieren. Die Angreifer geben sich dabei oft als vertraute Person oder Organisation aus, um das Opfer zu einer Handlung zu bewegen.

1 Vertrauen Sie nicht dem Anzeigenamen

Anzeigenamen können gefälscht werden. Prüfen Sie immer genau die E-Mail Adresse des Absenders. Auf Schreibfehler in der Domain achten.

2 Allgemeine / unpersönliche Anrede

Phishing Mails verwenden oft allgemeine Begrüßungen. Auch ungewöhnliche Grußformeln können ein Indiz für Phishing sein.

3 Nur schauen, nicht klicken

Hyperlinks können leicht manipuliert werden. Schauen Sie sich das Ziel eines Links genau an, bevor Sie es öffnen.

4 Anhänge nicht blind öffnen

Öffnen Sie keine Anhänge, welche Sie nicht erwarten. Auch Word, Excel und PDF Dateien können Schadcode enthalten, um Ihren Computer zu infizieren.

5 Rechtschreib- und Grammatikfehler

Phishing Mails enthalten oft Schreibfehler, da sie in fremder Sprache geschrieben und anschließend übersetzt werden.

6 Dringlichkeit und Zeitdruck

Wenn Sie aufgefordert werden, in einer kurzen Frist zu handeln, sollten Sie stutzig werden. Besonders in Verbindung mit Drohung von Konsequenzen.

7 Prüfen Sie die Signatur

Prüfen Sie ob die Signatur einer E-Mail dem gewohnten Schema entspricht. Falls nicht, kann dies ein Indiz für Phishing sein.

8 Die Frage nach sensiblen Daten

Angreifer fragen gezielt nach sensiblen Daten. Kein seriöser Absender wird Sie jemals nach Ihrem Passwort fragen.

9 Zu gut um wahr zu sein

Hinterfragen Sie stets den Inhalt einer E-Mail. Angreifer lügen oft um Ihr vertrauen zu gewinnen. Ist es zu schön um Wahr zu sein, ist es wahrscheinlich Phishing.

10 Im Zweifel die IT kontaktieren

Better safe than sorry! Im Zweifel wenden Sie sich immer zuerst an Ihre interne IT oder IT-Sicherheit.