Phishing Prevention/Detection User Guide

Phishing email messages, websites, and phone calls are designed to steal money and information. Cybercriminals can do this by installing malicious software on your computer or stealing personal information off of your computer.

Cybercriminals also use social engineering to convince you to install malicious software or hand over your personal information under false pretenses. They might email you, call you on the phone, or convince you to download something off of a website.

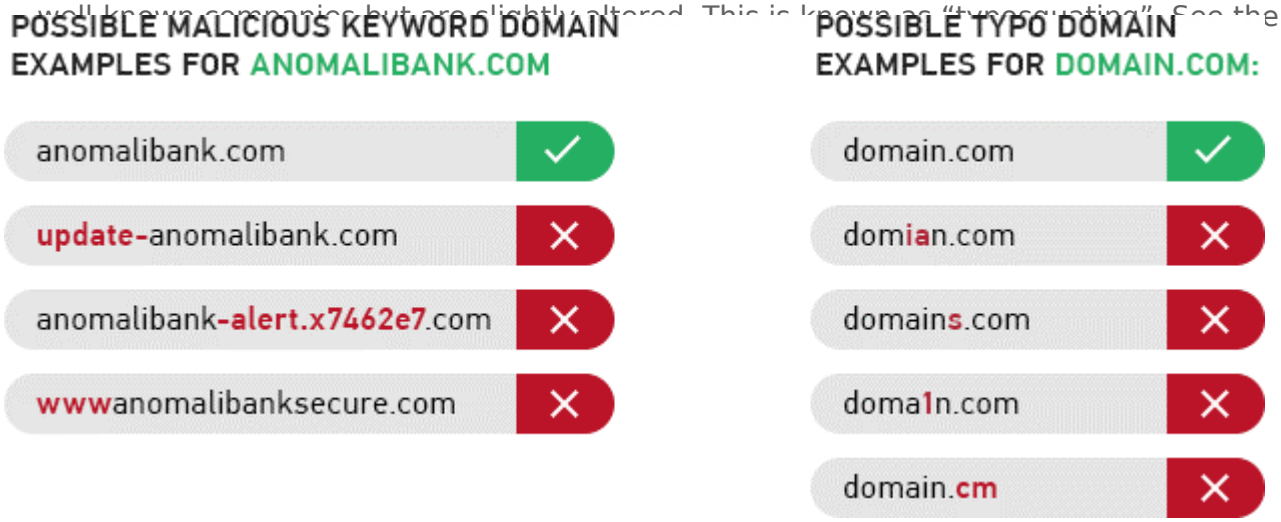
What does a phishing email message look like?

Here is an example of what a phishing email might look like:

- **Spelling and bad grammar -**Cybercriminals are not known for their grammar and spelling. Professional companies or organizations usually have a staff of copy editors that will not allow a mass email like this to go out to its users. If you notice mistakes in an email, it might be a scam.
- **Beware of links in email -**If you see a link in a suspicious email message, don't click on it. Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message. In the example below the link reveals the real web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's web address.

Links might also lead you to .exe files. These kinds of file are known to spread malicious software.

- **Threats and a send of urgency** -Have you ever received a threat that your account would be closed if you didn't respond to an email message? The email message shown above is an example of the same trick. Cybercriminals often use threats that your security has been compromised. For more information, see Watch out for fake alerts.
- **Spoofing popular websites or companies**- Scam artists use graphics in email that appear to be connected to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows. Cybercriminals also use web addresses that resemble the names of well-known companies but are slightly altered. This is known as "typosquatting". See the below



Beware of phishing phone calls

Cybercriminals might call you on the phone and offer to help solve your computer problems or sell you a software license. Neither Microsoft nor our partners make unsolicited phone calls (also known as cold calls) to charge you for computer security or software fixes.

Once they've gained your trust, cybercriminals might ask for your user name and password or ask you to go to a website to install software that will let them access your computer to fix it. Once you do this, your computer and your personal information is vulnerable.

Treat all unsolicited phone calls with skepticism. Do not provide any personal information.

Revision #1

Created 3 years ago by Biff

Updated 3 years ago by Biff