

What is a phishing attack?

In a classic phishing scheme, criminals try to dupe consumers into revealing personal information about themselves using fraudulent emails. Victims receive email purporting to be sent by a financial institution, or a prominent business (eBay is a frequent target, for example). Within the email are links to various websites, including valid links to the financial institutions web site, and links to the fraud artist's web site, which is designed to be identical to the users financial institutions site. When users "log in" to the false website, their login credentials are captured and can then be used by the criminals.

Variations on this attack include embedding malicious code such as a trojan horse or a spam bot into the site, and fake ecommerce sites that capture credit card information rather than login information.

Fortunately, phishing is a fairly well understood phenomenon on the internet today, and most browsers and many email clients incorporate anti-phishing features to protect users.

What is voice phishing, VoIP phishing, or vishing?

All three of those terms are names for the same thing – the use of a voice response system instead of a web site to dupe the unsuspecting consumer. Typically the crooks make a series of calls to the institution (such as a bank) that they're pretending to be, and record all of the prompts that the bank uses. They then construct an identical voice response system using a cheap telecom platform like the Open Source Asterisk platform.

Victims are sent either an email asking them to call an 800 number, or they receive a recorded message from the business that they patronize asking them to call an 800 number. The reason given is usually "to discuss your account", or some such. Then when the call is made, the victim may be instructed to enter credit card information into the telephone in order to "update your account". Very sophisticated criminals may answer the phone and ask the usual questions – name, address, date of birth, social security number – to confirm identity, and then ask for the credit card number. In either case, unsuspecting consumers expose themselves to identity theft.

Why is this a concern today?

The FBI has noted that criminal use of phone systems, and in particular phishing attacks, is on the rise. January 18th, 2008 they took the step of issuing a consumer warning about these kinds of attacks, instructing consumers about how to protect themselves.

At the same time, major American corporations such as AT&T and American Express are beginning to adopt the same technologies as a means to contain costs. AT&T, for example, often uses an autodialer to call customers, and instructs them to call an 800 number to speak with a representative "about an important issue concerning your account". The tactics that these corporations employ are identical to those that criminals employ. Whether through negligence, or simply a misunderstanding of the issue, corporate America is conditioning their customers to become victims of these scams.

How can consumers protect themselves?

Never contact a corporation you do business with in response to one of these solicitations. If you wish speak with a representative of the corporation, call the number on your statement, not the number left on your voicemail machine, or via email.

Do not give out personal information to others over the phone, unless you have initiated contact.

Inform businesses that you patronize that they do not have your permission to contact you via an autodialer. Demand that a human being call you, and be ready to provide information that will verify that they are in fact a representative of the business.

If a Do Not Call Registry exists in your country, add yourself to it. It won't screen out all telemarketing calls, but it will reduce the number and depending on the rules in your country, it may give you a clue as to the legitimacy of the caller.

What do you do if you've been defrauded?

1. Contact your credit card company, and inform them that your identity has been stolen.
2. Contact law enforcement and tell them that you've been a victim of fraud.
3. File a complaint with the Internet Crime Complaint Center - www.ic3.gov. This center is a joint venture between the FBI and the National White Collar Crime Center. In Canada, go to www.phonebusters.com or www.recol.ca.
4. Start a log of dates, person(s) that you spoke with and exactly what they said.
5. Contact the fraud departments of each of the two major credit bureaus.
 - a. Equifax: (877) 323-2598, for lost or stolen identification press 1, if you are a victim of identity theft press 2.
 - b. Trans Union: (877) 525-3823 except Quebec residents (877) 713-3393
6. Request that a "Fraud Alert" be placed in your files. At the same time order copies of your credit reports.
7. Contact the fraud department of creditors for any accounts that have been opened or tampered with fraudulently. This may include credit card companies, phone companies, banks and other lenders.

What steps can businesses take to protect their customers?

1. The obvious first step is to simply not make outbound autodialer calls. Conditioning consumers to avoid these types of calls is a great first step.
2. If you feel that outbound autodialer calls are a requirement for your business, then do not use them for solicitation of business. Use them only to discuss overdue bills with the customer. In addition, do not provide contact information in the call. Direct the recipient of the call to "call the toll-free number on your bill", or "visit our website to contact us".

3. When you are contacted by a customer, address the customer by name and provide verifiable personal information. Phone fraud artists don't ordinarily have access to this information.
4. Prominently publish numbers on your corporate web site so that customers can reach you by phone.

What can you do to make the businesses that you patronize aware of these issues?

1. Contact senior management of these corporations and let them know about this issue. Encourage them to abandon the use of autodialers.
2. Do not respond to autodialers. If you receive an autodialer solicitation, call or write to the VP of customer service, the VP of public relations, or the VP of Corporate Affairs at the corporation soliciting you, and explain why you don't wish to receive autodialer calls.
3. Write to the board of directors of the corporation, individually, and explain how the corporations actions are damaging the trust relationship that exists between the company and it's customers.
4. If do not call legislation exists in your country, determine whether it applies, and then submit a complaint. In the US, for example, corporations must respond to an FCC complaint, or risk a \$4000 fine, per incident.