Title:
How To Avoid Phishing And Spamming Online

Word Count:
535

Summary:
Phishing on AOL was closely associated with the warez community that exchanged pirated software. Those who would later phish on AOL during the 1990s originally used fake, algorithmically generated credit card numbers to create accounts on AOL, which could last weeks or possibly months. After AOL brought in measures in late 1995 to prevent this, early AOL crackers resorted to phishing for legitimate accounts.

A phisher might pose as an AOL staff member and send an instant m...

Keywords:
phishing, spamming, worms, trojans, web threats

Article Body:
Phishing on AOL was closely associated with the warez community that exchanged pirated software. Those who would later phish on AOL during the 1990s originally used fake, algorithmically generated credit card numbers to create accounts on AOL, which could last weeks or possibly months. After AOL brought in measures in late 1995 to prevent this, early AOL crackers resorted to phishing for legitimate accounts.

A phisher might pose as an AOL staff member and send an instant message to a potential victim, asking him to reveal his password. In order to lure the victim into giving up sensitive information the message might include imperatives like "verify your account" or "confirm billing information". Once the victim had revealed the password, the attacker could access and use the victim's account for criminal purposes, such as spamming. Both phishing and warezing on AOL generally required custom-written programs, such as AOHell. Phishing became so prevalent on AOL that they added a line on all instant messages stating: "no one working at AOL will ask for your password or billing information".

After 1997, AOL's policy enforcement with respect to phishing and warez became stricter and forced pirated software off AOL servers. AOL simultaneously developed a system to promptly deactivate accounts involved in phishing, often before the victims could respond. The shutting down of the warez scene on AOL

caused most phishers to leave the service, and many phishers—often young teens—grew out of the habit.

The capture of AOL account information may have led phishers to misuse credit card information, and to the realisation that attacks against online payment systems were feasible. The first known direct attempt against a payment system affected E-gold in June 2001, which was followed up by a "post-911 id check" shortly after the September 11 attacks on the World Trade Center. Both were viewed at the time as failures, but can now be seen as early experiments towards more fruitful attacks against mainstream banks. By 2004, phishing was recognized as a fully industrialized part of the economy of crime: specializations emerged on a global scale that provided components for cash, which were assembled into finished attacks.

Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Voice phishing sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

The damage caused by phishing ranges from denial of access to email to substantial financial loss. This style of identity theft is becoming more popular, because of the readiness with which unsuspecting people often divulge personal information to phishers, including credit card numbers, social security numbers, and mothers' maiden names. There are also fears that identity thieves can add such information to the knowledge they gain simply by accessing public records. Once this information is acquired, the phishers may use a person's details to create fake accounts in a victim's name. They can then ruin the victims' credit, or even deny the victims access to their own accounts.