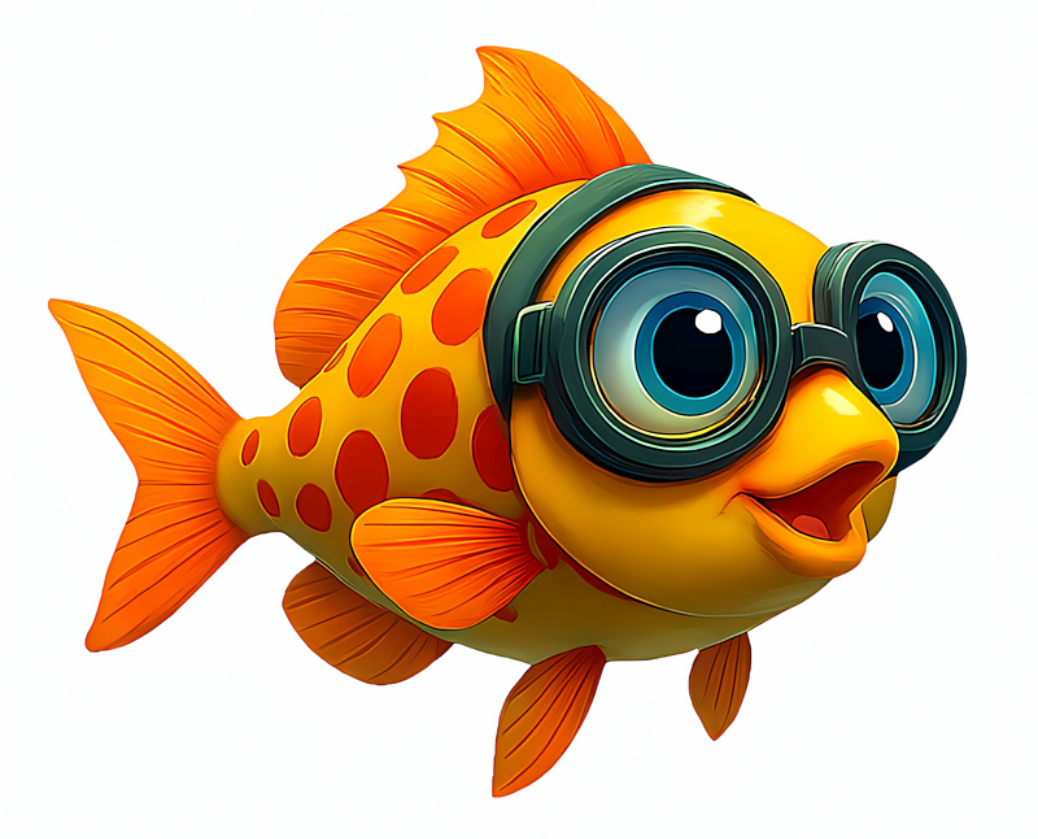
Science Translations
Established 1990
PC410.COM™
PC Updater News



How to Spot a Phish

Phish are evolving. In the past, large schools of phish were easily recognized as scams by looking for stupid stuff in the allegedly-urgent emails. There were spelling and grammar errors, capitalization errors that match other languages but not English, bad-logic lines like ‘in your nearest post office,’ and most important, the sending email address is some random international address that you don’t do business with. Logos of vendors were frequently out-of-date or distorted, and the links were clearly going to addresses ending in two-character country codes. AI is cleaning up those issues, and the phish are looking more like real business emails.

Basic Phish

Phish = A message that acts as bait, attempting to provoke a response that will start a login capture or a malicious download.

What the message says it is:

- A payment (How do they stuff dollar bills in an email?)
- An IRS letter (Those arrive by USPS mail)
- A website expiration or error message (for a free unlimited account, somehow)

Where that link goes:

- To a copy of a service login, but at a wrong and hacked page address (common)
- To a file-sharing service or web server, like Microsoft Azure or Docusign, or Amazon Web services, or lately, Adobe's document signing system.

What the message really is:

- A file containing a script that downloads software, that installs malware.
- A link to a look-alike copy of a bank or service login, that captures your login.
- A file containing a 'blob' web page, an offline copy of a login page, also for credential theft. The blob files are being used because they can get past a lot of security filters.
- A remote-access link. That's sometimes called a RAT, for Remote Access Trojan.

AI for Spear Phishing

AI systems are not smarter than humans. They are just faster. So smaller companies can be spear-phished. Before AI, most phishing messages were massively bland, and about as smart as a mail merge; they know the email address that the message is going to, and use the first half of that as the greeting name, and use your domain name as the company name. With spear phishing, previously seen as highly-targeted attacks against large companies, more specific information is in the message, like partner names, or company addresses and policies. Now, AI can look up details to insert into a spear phish message for anybody.

The More Things Change...

Your employees need to know this: You have established policies for payroll, banking, email management, and everything you do. A change in those policies that arrives with instructions to immediately take action in a new way has to be confirmed, and never by following the contact information in that message. Check with the boss, always and directly. Some industry groups are already major targets for this: broker/dealers and real-estate companies, or any company that routinely makes large onlne financial transfers.

It's still true that messages that ask you to do things in new ways, urgently, are generally fraudulent; large companies have a lot of inertia and don't often change how you log in or interact with them. They won't suddenly tell you to go to a third-party site like Docusign or Microsoft Azure or Amazon Web Services and download some important notice.

No major company that you want to do business with is splitting their login process into pieces over multiple services like that. When in doubt, go the main website of the company. Type their address into the browser; don't search for it. For the most-common example, go to bankofamerica.com rather than searching for 'bank of america'. You should know the web addresses of the financial institutions you use.

Similarly, know who you buy from. Keep a list. For example:

- For web sites, your domain name is from a registrar. It's probably Godaddy or Network Solutions or Wix (not a recommendation, but they have massive market share), or maybe at Spaceship.com or your web host.
- For web sites, your hosting company. If I run your web site, there are no automated warnings that require your action, ever. Elsewhere, pick up the

phone if you're not sure a message is valid.

- Online backup services. The most popular are Carbonite and Backblaze.
- Microsoft Office: It's at https://office.com and Microsoft is mostly getting rid of passwords now, so authentication is by web app or text messages or phone messages (all OK) or QR-code passkeys on a phone (not working properly yet–avoid this).
- And then there are the specialty online services that are industry-specific.

Unique Passwords Everywhere

These phish attempts are worse, much worse, for those of you who insist on using one password everywhere and forever. Again, once a phishing attack lands a password and user account login, or worse, an email login that can be used to confirm logins, these thieves will try using those logins at the top 20 to 50 banking and ecommerce sites, and see what accounts they get access to. AI will make this worse; AI software running on private systems has no ethical restrictions or practical roadblocks on logging into accounts it is told passwords for, and creating a list of successes. Those are followed up with transfers, gift card purchases, and other ways of putting your money to their use.

All online passwords must be unique. No repeats, no patterns, and nothing in the password that would show up in your online profiles, so no birthdays or

anniversaries, or names of children or pets, or prior addresses. Fixing one lost account is a nuisance but generally possible. Losing access to all your accounts because they shared one password takes years, with help from an account recovery company. Use unique passwords for anything online, always.

For computer help, call 410-871-2877
Missed a newsletter? Back Issues

Mailing address:
Science Translations
PO Box 1735
Westminster, MD 21158-5735