DON'T GET HOOKED BY A SCAM

Phishing is an email fraud method used by hackers and thieves. The email will appear to come from a legitimate sender in order to lure unsuspecting recipients into giving their personal, financial, or credential-related information. The scammers use that information to commit identity theft, gain access to your accounts, and even hack your computer.

Phishers are churning out much more convincing and effective emails. Not only are the most persuasive specimens well-written, they are also often personalized, addressing the recipient by name. In addition, they replicate the look and feel of authentic emails from legitimate businesses down to the fonts, footers, logos and copyright statements found in genuine company emails to customers or employees.

Phishers are becoming more sophisticated, so it's important that users become savvier at not getting hooked.

DID YOU GET HOOKED...

THERE IS HELP

We all make mistakes. If you believe you might have inadvertently revealed sensitive information such as a password, Social Security number, or financial account number, act fast to protect yourself.

1. Immediately change any passwords to accounts that were or could be affected.
2. If credit card information was exposed, immediately close that account, as well as any others that may be affected.
3. If your Social Security number was revealed, contact one of the three credit reporting agencies to place a fraud alert on your accounts. You should also consider purchasing credit monitoring.
4. File a police report.
5. Contact the spoofed company and alert them of the fraudulent email.

For additional resources go to:
security.arizona.edu/phishing
security.arizona.edu/idtheft

UA Information Security

security@arizona.edu
520.621.6700
security.arizona.edu

ALL ABOUT

PHISHING

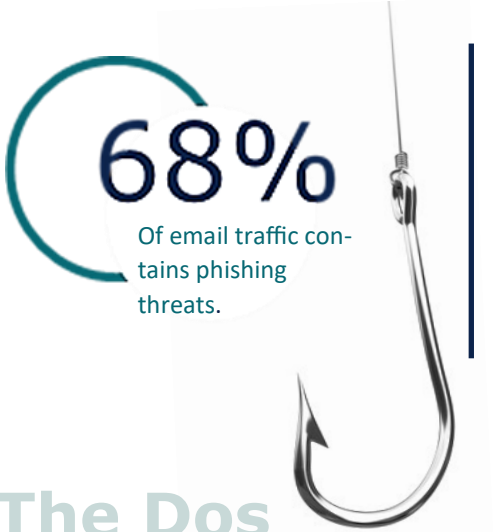
DON'T BITE

Information Security

HOW TO SMELL A PHISH

Phishers are social engineers, and social engineers are con artists. Here are tips for recognizing a phish:

1. **Sender tries to get you to act quickly before thinking.** The subject line will be alarming or enticing. Just remember, if it looks too good to be true, it is.
2. **Grammar and misspelled words.** Phishing emails often contain typos and poor grammar.
3. **Do the "hover" test: Is there a link in the email?** Hover over it with your mouse and see if the URL matches the one in the email. However, keep in mind that phishers are becoming more sophisticated in their scams, and may use web addresses similar to the correct link, (e.g., mybankonline.com instead of mybank.com).
4. **Sender requests sensitive information.** If you are asked to provide sensitive information, such as passwords or account numbers, either in an email or by clicking on a link, the email is a scam. NO legitimate business or organization (including the University of Arizona) will ask you to provide sensitive information in this way.
5. **The "reply to" address or sender's address does not match the company's URL.** If you receive an email claiming to be from your bank, a credit card company, or the University of Arizona, it should not be from an email address that you would not expect to find from the sending company (e.g., a Gmail, Hotmail or Yahoo! account).



Sign up for Phishing Alerts!

UA Information Security alerts campus about the latest phishing attacks on our website. Users can subscribe to the feed and receive alerts in their email inboxes. Go to security.arizona.edu/phishing-alerts.

The Dos
The Don'ts
The Nevers

Help Us Help UA: Report that Phish!

Did you receive a phish that you don't find in the alerts? Report the phish to our office at: phish@arizona.edu

1. **DO be patient and think before you act.**
   - Too many users end up the victims of Internet crime because they do not stop to think, but instead act on impulse, clicking on a "sexy" link or an interesting looking attachment without thinking of the possible consequences.
2. **NEVER respond to unsolicited email, or supply personal or log-in information.**
   - No one should ever request that you provide your credentials or other sensitive information unless YOU initiated the contact.
3. **DON'T click on any links in emails.**
   - Never follow any embedded links. Instead, double-check URLs by visiting a company's website via a Google search or another independent method.
4. **DON'T open unexpected attachments.**
   - Contact the email sender to verify the contents.
5. **DO regularly check statements from your accounts.**
   - If you notice any suspicious transactions, report them immediately to your bank or credit card provider.
6. **NEVER share your passwords or PINs.**
   - Do not write them down, and do not use the same password for all your accounts.
7. **DO keep your computer secure.**
   - Install anti-malware software, and sign up for automatic updates. Sign up for automatic updates for all software installed on your computer.
8. **DO report suspicious activity.**
   - If you receive an email you suspect isn't genuine, alert the spoofed organization.