Internet Scams & Phishing

Sam Duncan, Maryl Gearhart, and Hilary Naylor

with Pat Hom, Celie Placzek, and Craig Griffith

Ashby Village Technology Volunteers

This Tech Tip provides information on common phishing scams and their features. We then give you tips on what to do if you receive a phishy email or if a phishy browser window pops up, and how to minimize the risks from phishing scams.

What is "phishing"?

Let's begin with a basic definition. The term "phishing" captures the idea of "fishing for information" or "fishing for money," and then "hooking" the victims. In a typical scam, internet fraudsters send an e-mail to trick unsuspecting victims into sending money, or revealing personal and financial information. You might receive an email from a 'relative' who claims to be in trouble and needs money immediately. Or you might receive an email from the "Internal Revenue Service" informing you of a tax refund, and asking you for your social security number. Or, when you're online, you might see a window pop up telling you that your computer needs repair, and asking you to type in personal information and send money.

Email scams & phishing

The most common internet phishing attempts are via email, and there are many types of email phishing attempts. We summarize some common types first and then highlight common features,

<u>Common types of email phishing</u>

- *Urgent requests* appear to be from a company you trust, like Netflix, your bank, or Costco. The email states that your account has been suspended, and you must reactivate *now* by clicking and entering account or financial information.

- *Unexpected refunds, payments, or rewards are* simply too good to be true! You're offered a tax refund or a reward if you click and enter personal information. These offers are often "time-limited" and urge you to respond immediately.

- *Come-ons invite* you to participate in a survey or contest by clicking and entering personal information.

- *Requests for money are* fraudulent requests for help with emergencies from strangers or from fraudsters posing as relatives, friends, charities, police, etc. The emailer may plead, "I'm stuck in London!" "I'm out of money!" "I'm in jail!" "I was in an accident!" Often the amount requested is small to encourage you to believe the request is reasonable and legitimate.

Common features of email phishing attempts

- *Counterfeit logo and graphics*: The email appears to be from a company or agency you trust. But while the logo and graphics initially appear genuine, a closer look reveals that they're counterfeits.

- *Bogus email sender*: If you hover your cursor over the email sender, you discover the email is not from the trusted company or agency. For example, a phishing email from "Netflix" might actually be from "@godaddy.fr," obviously not Netflix. Sometimes the sender is very close to the authentic spelling, e.g., "@Netflicks" rather than "@Netflix."

- *Errors in spelling or grammar and/or unprofessional formatting:* Phishing emails often have typo errors or unprofessional formatting. In contrast, emails from a trusted company or agency are carefully prepared and edited.

- *Generic greeting*: A phishing email typically greets you with "Hello" or "Dear Customer" rather than your name.

- *Generic reference to your account:* The email typically refers to "your card" or "your account" with no reference to your unique account. Legitimate emails are more likely to include the last four digits of your account number ("xxxx xxxx xxxx 4321").

- *Conveys urgency, with a request to click*: Phishing emails often convey urgency and ask you to click *now* to resolve a problem or claim a time-limited offer.

Browser pop-up phishing attempts

Your browser is the application you use to use the internet - for example, Chrome, Firefox, or Safari. Phishing attempts can suddenly appear in pop-up windows in your browser, and we highlight two common types.

Types of browser pop-up scams

- *Your computer needs repair:* This type of pop-up window informs you that your computer needs immediate repair. Sometimes the pop-up provides specific information that appears to be convincingly authentic, such as "Your computer is heavily damaged (32%)" or "Your computer is infected with 3 viruses." The pop-up may urge you to click or call to provide further information and payment for repair. Or the pop-up may recommend that you "scan now" to clean your computer, but unfortunately if you click the "scan now" link, you download malware onto your computer. *Rest assured that Apple, Microsoft, and other tech companies will NEVER post a threatening pop-up about computer repair.*

- *Ransom demanded:* Another type of browser pop-up scam is "ransomware" -- you're told your computer has been seized, and you must pay a ransom to access it. Fortunately, everyday computer users rarely experience ransomware attacks; ransomware is generally directed to organizations and businesses.

Common features of scams in browser pop-up windows

The features of pop-up scams are similar to the features for phishing emails, so please review the earlier information under "Email scams and phishing."

- *Counterfeit logo and graphics*
- *Errors in spelling or grammar, and/or unprofessional formatting*
- *Generic greeting* rather than your name
- *Generic reference to your account*
- *Conveys urgency, with a request to click*

What to do when you're concerned

From time to time we all receive phishing emails or confront a browser pop-up window. What should you do if you're concerned?

Be cautious

- *First, think before you act - there is no rush!* Step away from your computer (sit down and have a cup of coffee!).
- *If in doubt about email:* Move the email to your email client's Spam or Junk folder to help your system learn what you regard as unwanted email.
- *If in doubt about a pop-up window:* Delete your browser history, close your browser, and restart your computer.
- *Investigate:* Look at company or agency website - are they actually offering or requesting something? Consider contacting the company or agency to inquire and report the email or pop-up.

<u>If you clicked a suspicious link</u>

We've all done it - we've clicked a link in a suspicious email. Please don't panic, and don't be embarrassed!

Here's our advice:

- *If it's an email scam:*
    - *Document* - take a photo or a screenshot, or write down what you see on your screen.
    - *Change passwords* for your email and the relevant accounts (e.g., Netflix if it's a Netflix phishing email).
- *If it's a browser pop-up about computer repair:*
    - *Document* - take a photo or a screenshot, or write down what you see on your screen.
    - *Delete browser history, close your browser, and restart your computer.*
- *If it's a browser pop-up demanding ransom payment:*
    - *Document* - take a photo or a screenshot, or write down what you see on your screen.
    - *Do nothing more* - do not touch any buttons.
    - *Request immediate help from a tech professional.*
- *If you've shared financial information:*

- *Document* - take a photo or a screenshot, or write down what you see on your screen.
- *Contact your financial institution to close the account.*
- *Watch for unauthorized charges.*
- *Consider filing a report to police.*

How to minimize your risks

We all want to reduce the frequency of phishing attempts, and minimize the risks when we're 'phished.' What to do? We have a number of recommendations.

- *Update regularly:* Update your operating system, your browsers, and your applications regularly. (Browser examples are Safari, Chrome, and Firefox.) Updates are important because each update includes security features that help to protect your computer from the latest malware.
- *Back up regularly.* Regular backup is very important! If you inadvertently click on a link that downloads malware onto your computer, you need your backup to restore your computer to its previous virus-free state.
- *Use complex passwords, and use different passwords for each account.* If you use the same password for many accounts, a phisher who captures the password to one account can then open other accounts. To minimize risk, use different passwords for each account! Store your password records in a safe location, and remember to update your records whenever you change a password. *Consider using a password manager application to generate and store your passwords. Examples include 1Password, LastPass, Dashlane, and Keeper.*
- *Mark suspicious emails as junk/spam.* When you move suspicious email to Junk or Spam, you help teach your email client what you regard as spam or scams.
- *Block pop-up windows on browsers.* Browser preferences allow you to block pop-up windows entirely or selectively. Please request assistance if you're uncertain how to modify the pop-up preferences for your browser (e.g., Chrome, Firefox, Safari).

Final comment

Computers, smartphones, and tablets are wonderful tools. They open the doors to the outside world by providing links to people, places, and ideas we never would have imagined! While the benefits of internet access far outweigh the risks, it's important to be mindful. We hope that our tips will better equip you to enjoy the virtual world without being anxious.

Ashby Village volunteers are available to help you!

If you need technology assistance at any time, email info@ashbyvillage.org or call 510-204-9200 to request a technology volunteer.