

Webex: Tips to Protect Your Identity

Office of Information Security (OIS)

Office of Technology Services (OTS)

October 17th, 2019



Tips to Protect Your Identity at Home

- Establish Text Alerts to help Fight Fraud
- Run an Antivirus scan periodically
- Enable 2 factor authentication on personal accounts
 - Configure Privacy and Security and Login settings
- Report Phishing and Spam
 - Forward Text Scams to 7726 (SPAM)
- Create strong passwords
- Secure your connection – Look for HTTPS
- Keep devices and computers up to date

2 Factor Authentication – Facebook

<https://www.facebook.com/security/2fac/setup/intro/>




Facebook

facebook.com/security/2fac/setup/intro/

Search

Joel Home Create

Two-Factor Authentication > Two-Factor Authentication





Add Extra Security With Two-Factor Authentication

Help protect your account, even if someone gets hold of your password.

[Get Started](#)

How Two-Factor Authentication Works

 **Extra Protection**
If we notice a login from a device we don't recognize, we'll ask for a login code before you can access your account.

 **Through SMS or an Authentication App**
We'll send a text message with a login code, or you can use a security app of your choice.

About Create Ad Create Page Developers Careers Privacy Cookies Ad Choices Terms Help

Facebook © 2019
English (US) Español Français (France) 中文(简体) العربية Português (Brasil) Italiano 한국어 Deutsch हिन्दी 日本語 +

Report Phishing and Spam – Personal Outlook

The screenshot shows the Outlook interface with a blue header bar containing the 'Outlook' logo and a search bar. Below the header is a navigation bar with icons for 'New message', 'Delete', 'Archive', 'Junk', 'Sweep', 'Move to', and 'Categorize'. The left sidebar displays 'Favorites' (Inbox: 33374, Sent Items: 1, Drafts: 1) and 'Folders' (Inbox: 33374, Junk Email: 146, Drafts: 1, Sent Items: 1, Deleted Items: 2, Archive, Conversation History, Notes: 2, Phishing Awareness E..., New folder). The main content area shows an email from 'Congratulations <fsdgrehygsdxg@j5YJo.baratheonboltons.com>' dated 'Mon 9/30/2019 5:29 AM'. The email body features a large black Amazon gift card with '\$1000' and the Amazon logo. Below the card, it says 'Take this 30 second survey about Amazon and we'll offer you a \$1000 exclusive reward.' and includes a 'Click here to get started' link. At the bottom, there is a disclaimer: '*PURCHASE REQUIRED. SEE OFFER FOR DETAILS. This advertisement was sent to you by a third party. If you are not interested in receiving future RewardZoneUsa advertisement, please Click Here. Alternatively, you can opt out by sending a letter to: RewardsFlow, LLC 128 Court Street, 3rd FL White Plains, NY 10601.' A right-hand menu is open, showing options like 'Reply', 'Delete', 'Mark as phishing', and 'Block Congratulations'. The 'Phishing Awareness E...' folder in the sidebar is highlighted.

Report Phishing and Spam – Personal Gmail

Updated FollowMyHealth Terms of Use and Privacy Policy Spam x

FollowMyHealth noreply@followmyhealth.com via sendgrid.net
to me

Thu, Oct 17, 11:43 PM (4 days ago)

Why is this message in spam? It is similar to messages that were identified as spam in the past.

[Report not spam](#)

Reply
Forward
Filter messages like this
Print
Delete this message
Block "FollowMyHealth"
Report phishing
Show original
Translate message
Download message
Mark as unread

Hello,

The FollowMyHealth team has been working hard to add new features and services in order to improve your user experience. Today, we're emailing you to let you know about updates to our Terms of Use and Privacy Policy.

You may have noticed we updated our [Terms of Use](#) and [Privacy Policy](#) to provide more clarity about using FollowMyHealth, to address new features and functionality, and to include other updates and clarifications.

We encourage you to read our updated Terms of Use and Privacy Policy in full, but here are the high-level changes:

- How we collect, use, and disclose your information
- How we protect the security of your information
- How we may use and disclose your information for marketing or advertising purposes
- How we may display advertising or marketing to you while you use FollowMyHealth
- The manner in which FollowMyHealth may communicate with you

These terms went into effect for all users on August 14, 2019. Please be aware that by continuing to use FollowMyHealth, you acknowledge and agree to the updated Terms of Use and Privacy Policy. If you do not agree to the updated Terms of Use and Privacy Policy you can delete your FollowMyHealth account at any time. The Terms of Use are to be read in conjunction with the Privacy Policy, which is incorporated into the Terms of Use and forms part of our contract with you.

If you have any questions, please let us know.

support@followmyhealth.com

Copyright© 2019 Allscripts, All rights reserved.

You're receiving this email because you have a FollowMyHealth® account or agreed to receive emails from your healthcare provider who uses FollowMyHealth®.

Our mailing address is:
222 Merchandise Mart
Chicago, IL 60654

Secure your connection – Look for HTTPS



A screenshot of a web browser displaying the Towson University website. The browser's address bar shows 'towson.edu' with a lock icon on the left, indicating a secure connection. A notification box on the left side of the browser window states 'Connection is secure' and provides information about data privacy. The website header includes the Towson University logo and navigation links for 'TIGER ATHLETICS', 'SUPPORT TU', and 'QUICK LINKS'. Below the header is a yellow navigation bar with categories like 'ACADEMICS', 'ADMISSIONS & AID', 'STUDENT LIFE', and 'CAMPUS & COMMUNITY'. The main content area features a large image of a football player in mid-air, with the URL 'https://staysafeonline.org/' overlaid in yellow. Below the image is a headline 'Finding his home as a Tiger' and a 'Read More' button. At the bottom, there is a yellow bar with the text 'FIND YOUR AREA OF STUDY' and dropdown menus for 'UNDERGRADUATE PROGRAMS', 'GRADUATE PROGRAMS', and 'OTHER PROGRAMS'. The page concludes with the heading 'Get to Know TU' and a row of three small images.

Free Resources



Have I been Pwned: <https://haveibeenpwned.com>



The screenshot shows the homepage of the Have I Been Pwned website. At the top, there is a navigation menu with links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is a large white box containing the text ';--have i been pwned?'. Below this is a sub-heading: 'Check if you have an account that has been compromised in a data breach'. A search input field labeled 'email address' is followed by a 'pwned?' button. Below the search area, there is a promotional banner for 1Password: 'Generate secure, unique passwords for every account' with a link to 'Learn more at 1Password.com'. The footer section displays four statistics: 409 pwned websites, 8,506,944,706 pwned accounts, 102,441 pastes, and 122,480,433 paste accounts. It also features two columns of breach information: 'Largest breaches' and 'Recently added breaches', each listing the number of accounts affected and the name of the breach.

Category	Value
pwned websites	409
pwned accounts	8,506,944,706
pastes	102,441
paste accounts	122,480,433

Category	Accounts	Breach Name
Largest breaches	772,904,991	Collection #1 accounts
	763,117,241	Verifications.io accounts
	711,477,622	Onliner Spambot accounts
	593,427,119	Exploit.In accounts
	457,962,538	Anti Public Combo List accounts
Recently added breaches	71,407	Zooville accounts
	988,230	StreetEasy accounts
	780,073	Sephora accounts
	23,165,793	Wanelo accounts
	15,453,048	Lumin PDF accounts

Password Check: <https://password.kaspersky.com>

English

kaspersky

SECURE PASSWORD CHECK

⚠ Never enter your real password
This service exists for educational purposes only - Kaspersky is not storing or collecting your passwords.

Test your password *

kaspersky

© 2019 AO Kaspersky Lab. All Rights Reserved.
[Privacy Policy](#)

Jigsaw | Google Phishing Quiz : <https://phishingquiz.withgoogle.com>

The screenshot shows a web browser window with the URL phishingquiz.withgoogle.com. The page has a blue background and features the following content:

- A language selector at the top center showing "English (United States)".
- The main heading: "Can you spot when you're being phished?"
- A sub-heading: "Identifying phishing can be harder than you think. Phishing is an attempt to trick you into giving up your personal information by pretending to be someone you know. Can you tell what's fake?"
- A blue button labeled "TAKE THE QUIZ".
- An illustration of a yellow hand holding a fishing hook.
- A footer with the "Jigsaw | Google" logo on the left and "Privacy / Terms / Feedback" links on the right.



Question & Answers



- Email questions to **securityawareness@towson.edu**
- If you would like an OIS team member to give an interactive phishing or security awareness presentation to your group or department, please visit **<https://towson.edu/securityawareness>**.

Thank You for Attending Today's NCSAM Webex Event

